NETWORK INTELLIGENCE

ISO 27001 CERTIFIED | PCI DSS QSA

Security Operations Center

MUM-CT-1076

TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Introduction to SIEM

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

- What is SIEM ?
  - Security Information and Event Management is a combination of two different types of Technologies.
  - **SIM (Security Information management)** - Log collection and Report generation
  - **SEM (Security Event management)** – Analysis of Event in Real-Time and correlation of events.

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Capabilities of SIEM

- Aggregation of Data
- Alerts
- Correlation
- Analyse
- Retention
- Scalability

© Institute of Information Security

Introduction to SIEM

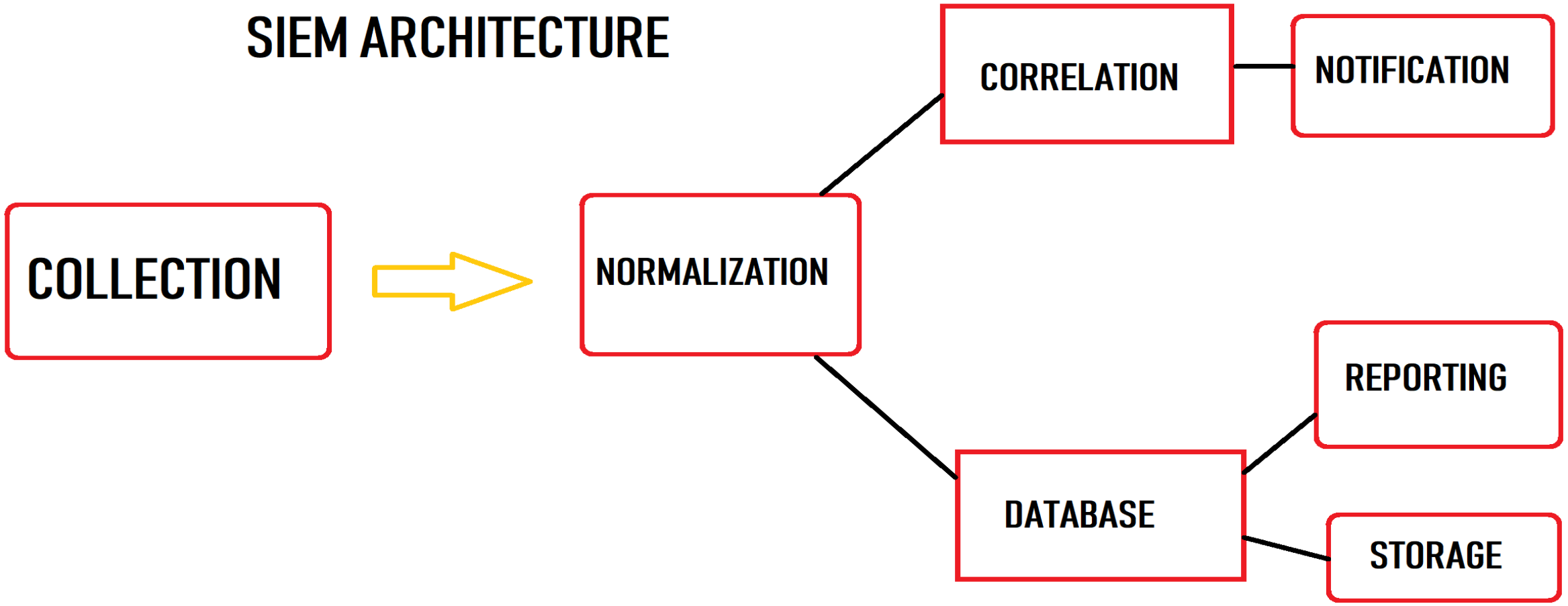
NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Why do we need SIEM?

- Rise in Data breaches due to Internal and External Threats
- Attackers are Smart & Traditional security tools just don't suffice
- Mitigate Sophisticated Threats.
- Manage increasing volume of Logs from multiple sources
- Meets stringent compliance requirements

© Institute of Information Security

SIEM Architecture



© Institute of Information Security

SIEM Architecture

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Collection – Logged Data is collected from all Network devices such as computers, Servers, Switches, Routers for analysis and investigation.

Normalization – Redundant Event Log entries, which are collected from thousands of devices are eliminated and the collection is made more precise

Correlation – The Redundant Log data is looked for some common patterns between data from different sources to find some link between them.

Database – Logs are retained in the database if they are not processed quickly enough by server. They can be retained for 90 days

© Institute of Information Security

SIEM Architecture

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Notification – Alarms are raised in real-time as when predefined rules are met.

Reporting – Reporting events or Incidents in the detailed reports on current security posture of all Network devices, is generated and shared with senior management for decision making on Security Investment

Storage – Storing Events logs for long period of time, for future reference to facilitate correlation of data over time.

© Institute of Information Security

User Behaviour Analysis

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

The User Behavior Analytics is a tool for detecting insider threats in your organization.

Risk profiling

Risk is assigned to each one depending on the severity and reliability of the incident detected.

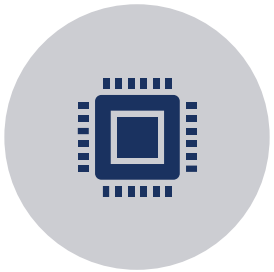
UBA uses existing event and data in your SIEM system to generate these insights and profile risks of users.

To generate these Insights, Data from EDR, SaaS, Proxies, Firewalls, IPS, VPN

© Institute of Information Security

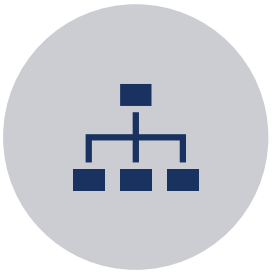
Network Behaviour Analysis

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA



ANALYZE NEW MALWARE STRAINS

PERIMETER SECURITY



BEHAVIORAL ANALYSIS

FEEDING DATA FROM NETWORK DEVICES

© Institute of Information Security

QRadar

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

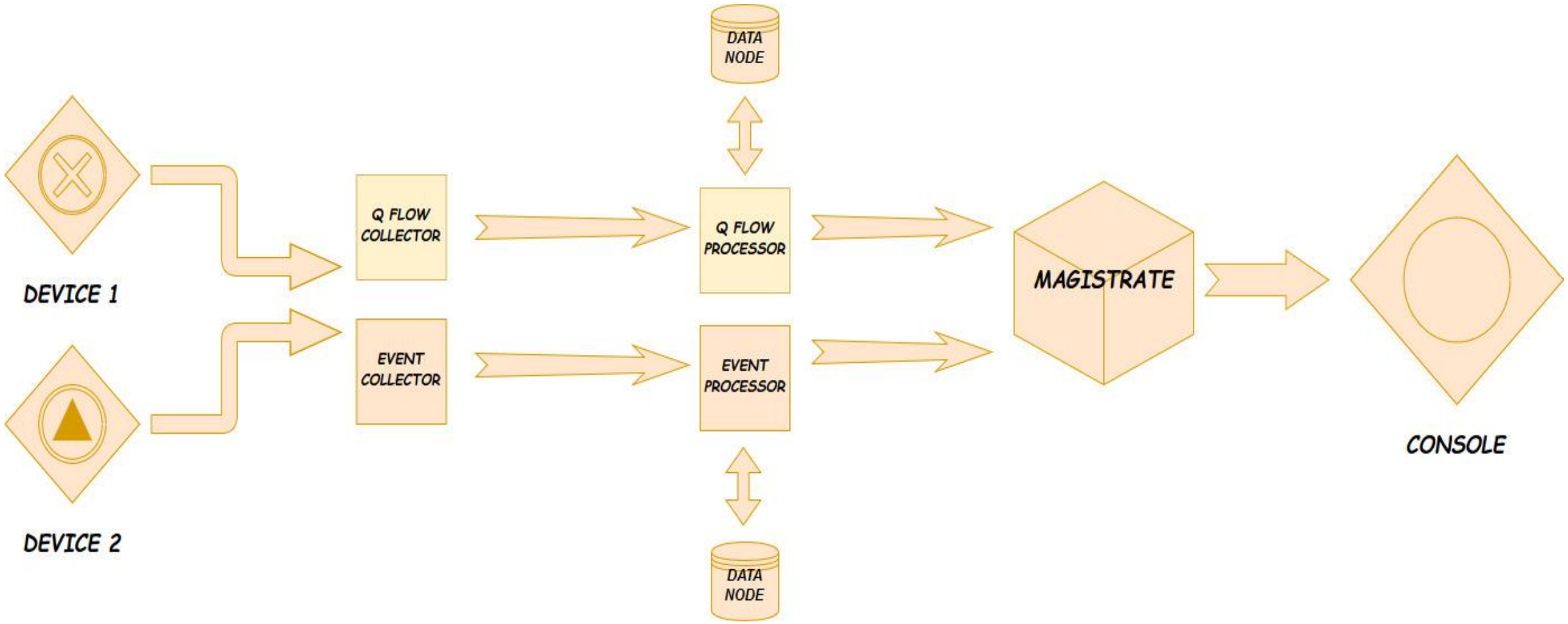
Qradar is a SIEM solution, formerly developed by Q1 Labs but is now owned by IBM after its acquisition, in 2011

Gartner has rated Qradar as the Leading Information Security Intelligence and Analytics platform

What makes QRadar standout from its competitors, is the incorporation of Automation in detecting Log sources and The option to Integrate Watson (IBM's AI).

© Institute of Information Security

QRADAR Architecture



© Institute of Information Security

QRadar

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

QRadar Console

- Provides Interface for QRadar product. Interface delivers real-time event flow views, reports, offenses, asset information and administrative functions.
- QRadar Console is efficient while in a distributed QRadar deployments, to manage hosts and other components.

QRadar event Collector

- Gathers events from local and remote Log sources. Normalizes raw log events. On the Backend Magistrate examines the events from log and maps event to a Qradar Identifer .

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Qradar Qflow Collector

- Passively collects traffic flows from the Network through Span ports or Network Taps.
- Qradar Qflow Collector is capable of collecting External flow-based data sources, such as NetFlow.
- Qradar Qflow collectors can be installed on the device or just use one of existing applicances.

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

QRadar Event Processor

- Processes Events which are collected from one or more Event collectors.
- Event processor correlates the information form QRadar products. It also feeds the processes events to appropriate destinations. You can choose to skip over Qradar Collector and feed logs directly to Qradar Processor, if needed.
- Event processors also store information related to Behavorial changes or policy violations for events, collected across different Qradar products
- Once its completed processing events, it feeds the results to Magistrate

© Institute of Information Security

QRadar

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Magistrate/Console

- Provides all the core processing components. Magistrate provides views, reports, alerts and analysis of Network Traffic and Security Events.
- Magistrate processes events against existing custom rule set. If and Event matches a rule, Magistrate component generates the response configured in the custom rule.

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Data Node

- These are primarily used for storage purposes.
- They are a on-demand type of service.
- They help increase the processing and storage capacity, by providing more hardware resources.

© Institute of Information Security

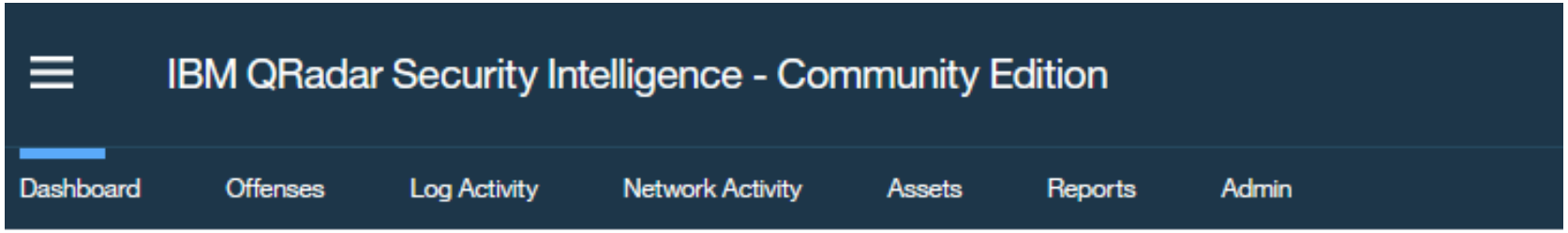
NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

QRadar Tabs

- **Dashboard** – The Comprehensive overview
- **Offenses** – Displays Offenses, Alerts, Incidents
- **Log Activity** – Query and display events
- **Network Activity** – Query and display flows
- **Assets** – Query and display information about systems in the network
- **Reports** – Create Templates and generate reports
- **Admin** – Administrative management tools

© Institute of Information Security

Qradar Tabs - Practical



MUM-CT-1076
TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Offenses

- QRadar automates detection of suspicious activity and ties them together into a offense
- Offenses Tab provides functionality of Investigating a triggered Offense
- Some examples of Offense –
  - Multiple Login Failures
  - Malware Infection
  - Suspicious Server

© Institute of Information Security

QRadar

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

QRadar creates a Offense when specific thresholds for event, flow or both are met, these are customizable rules.

For this QRadar Analyzes following information

Magistrate rates each Offense within range on 1 – 10

- Incoming Events and Flows
- Asset Information
- Known Vulnerabilities

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Offense Tab

- Offense Parameters
- Offense Source Summary
- Last 5 Notes
- Last 5 source Ip's
- Last 5 Destination Ip's
- Top 5 Log sources
- Top 5 Users
- Top 5 Categories
- Top 10 Events
- Top 10 Flows
- Top 5 Annotations

© Institute of Information Security

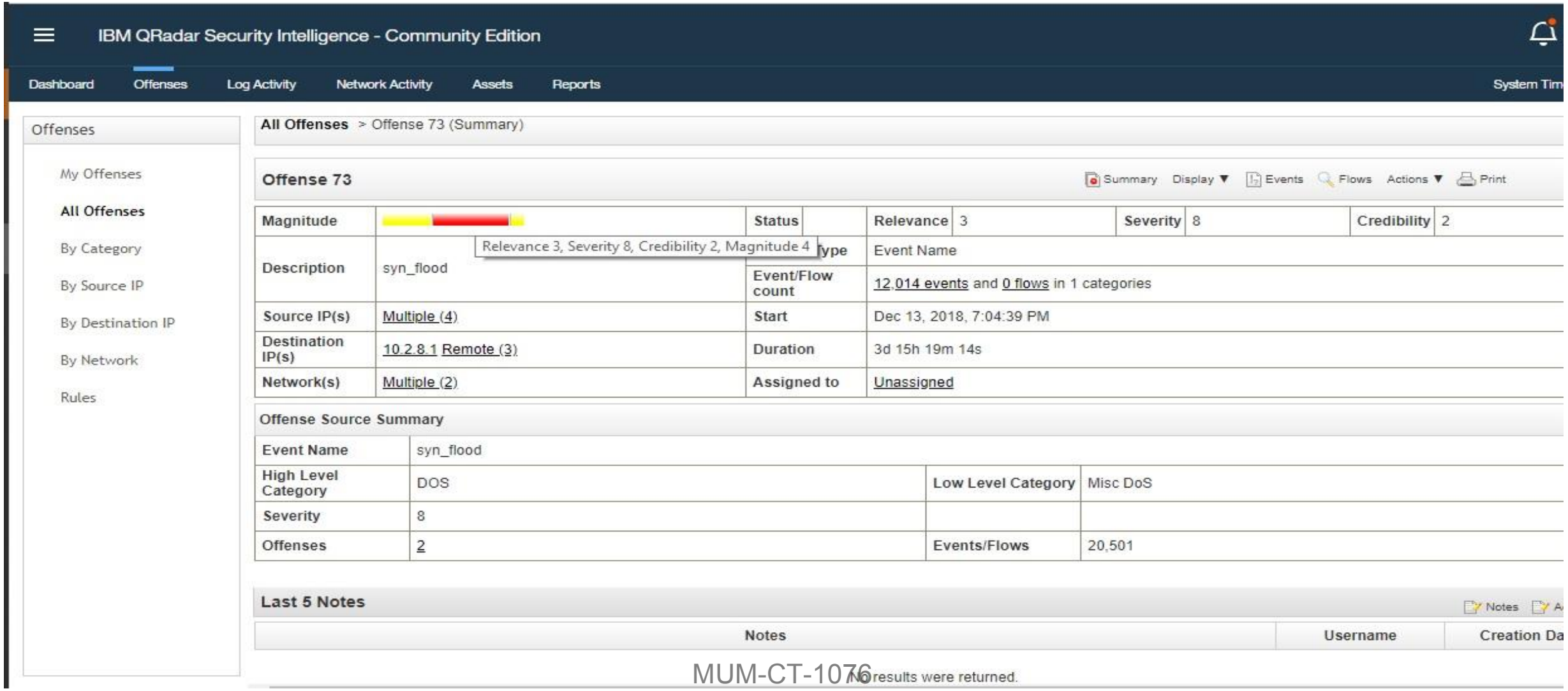
NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Offense Parameters

- **Magnitude** – Prioritizes offenses as per the importance.
- **Status** – The Offenses on the slide are Active
- **Relevance** – Indicates the importance of where the Offense has occurred, Lesser important areas in a Network would have lower relevance
- **Severity** – The Intensity of Threat an attack poses, calculated in relation to vulnerability of destination
  - **Credibility** – Indicates the reliability of the Offense based on witnesses, more witness , higher the credibility

© Institute of Information Security

Offense - Magnitude



© Institute of Information Security

Practical Session

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

MUM-CT-1076
TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Offense Types

- Event name
- Source IP
- Source Port
- Source MAC address
- Destination MAC address
- Destination IPv6
- Username
- Log Source
- Destination Port
- Source IPv6 and many more

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

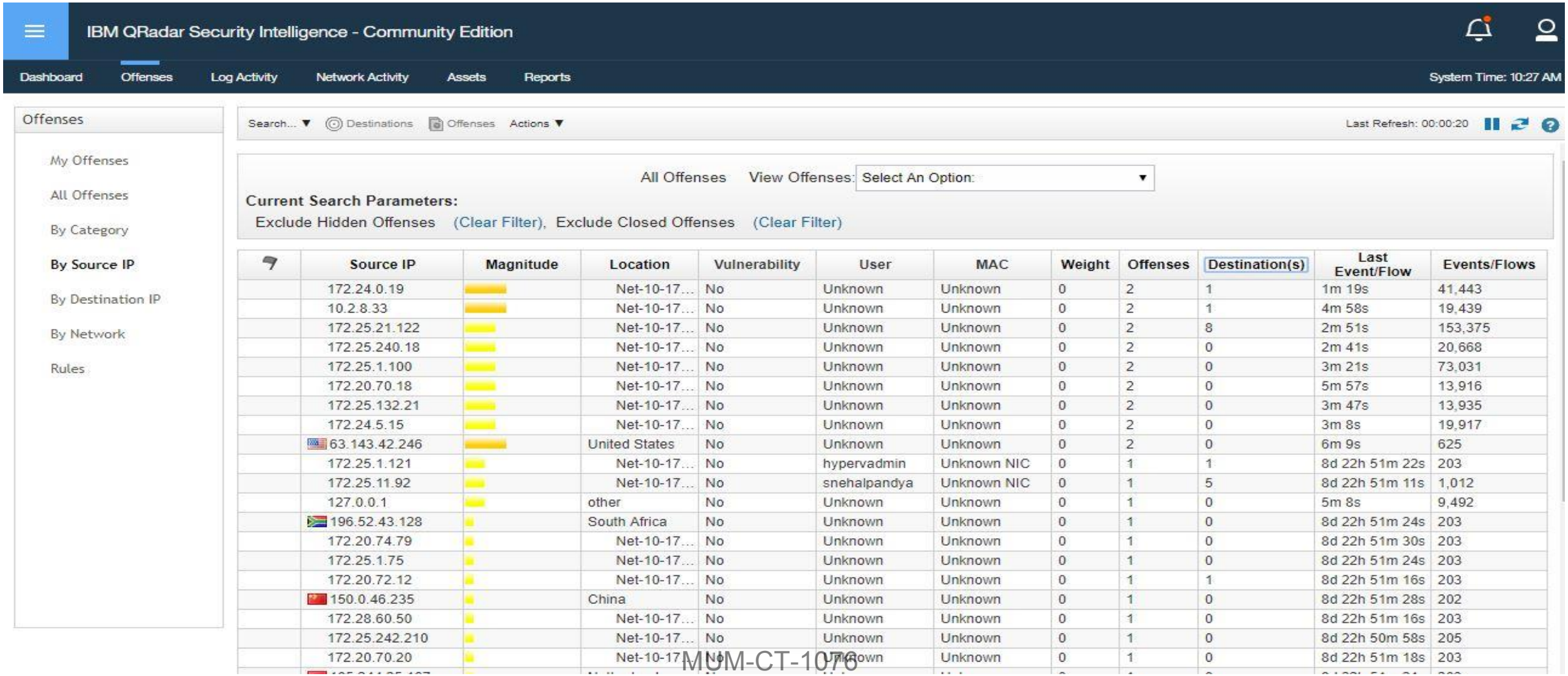
Further detailed Offense Parameters

- Source IP's – If the Offense was triggered from a single IP, it will be displayed, but if multiple IP address are involved it can be accessed through Multiple(n)
- Destination IP's – If Offense has only one Target its IP address is displayed, but if it has multiple IP addresses following notation are used
  - **Local**(n) – Local IP addresses if targeted
  - **Remote**(n) – Remote IP addresses if targeted

© Institute of Information Security

Offense – Source IP

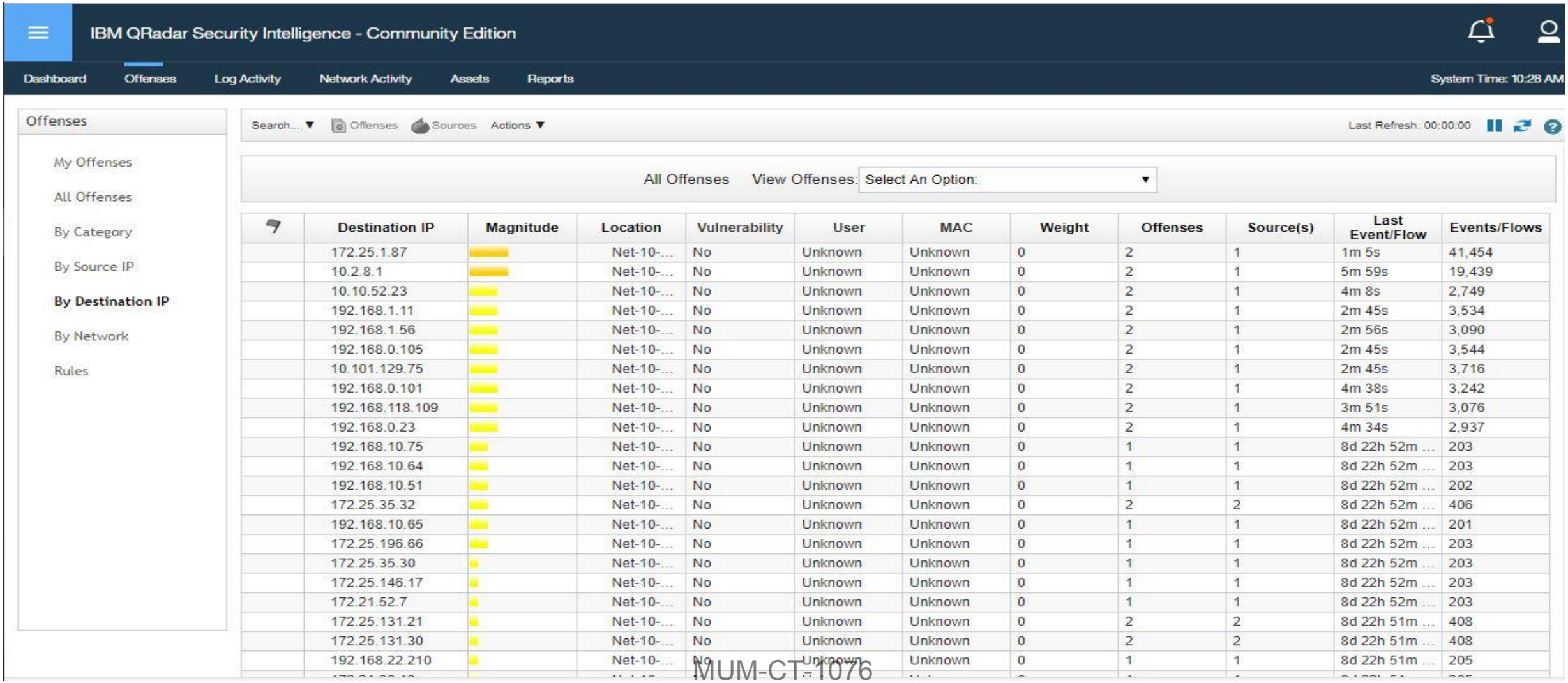
NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA



Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
172.24.0.19		Net-10-17...	No	Unknown	Unknown	0	2	1	1m 19s	41,443
10.2.8.33		Net-10-17...	No	Unknown	Unknown	0	2	1	4m 58s	19,439
172.25.21.122		Net-10-17...	No	Unknown	Unknown	0	2	8	2m 51s	153,375
172.25.240.18		Net-10-17...	No	Unknown	Unknown	0	2	0	2m 41s	20,668
172.25.1.100		Net-10-17...	No	Unknown	Unknown	0	2	0	3m 21s	73,031
172.20.70.18		Net-10-17...	No	Unknown	Unknown	0	2	0	5m 57s	13,916
172.25.132.21		Net-10-17...	No	Unknown	Unknown	0	2	0	3m 47s	13,935
172.24.5.15		Net-10-17...	No	Unknown	Unknown	0	2	0	3m 8s	19,917
63.143.42.246		United States	No	Unknown	Unknown	0	2	0	6m 9s	625
172.25.1.121		Net-10-17...	No	hypervadmin	Unknown NIC	0	1	1	8d 22h 51m 22s	203
172.25.11.92		Net-10-17...	No	snehalpandya	Unknown NIC	0	1	5	8d 22h 51m 11s	1,012
127.0.0.1		other	No	Unknown	Unknown	0	1	0	5m 8s	9,492
196.52.43.128		South Africa	No	Unknown	Unknown	0	1	0	8d 22h 51m 24s	203
172.20.74.79		Net-10-17...	No	Unknown	Unknown	0	1	0	8d 22h 51m 30s	203
172.25.1.75		Net-10-17...	No	Unknown	Unknown	0	1	0	8d 22h 51m 24s	203
172.20.72.12		Net-10-17...	No	Unknown	Unknown	0	1	1	8d 22h 51m 16s	203
150.0.46.235		China	No	Unknown	Unknown	0	1	0	8d 22h 51m 28s	202
172.28.60.50		Net-10-17...	No	Unknown	Unknown	0	1	0	8d 22h 51m 16s	203
172.25.242.210		Net-10-17...	No	Unknown	Unknown	0	1	0	8d 22h 50m 58s	205
172.20.70.20		Net-10-17...	No	Unknown	Unknown	0	1	0	8d 22h 51m 18s	203

© Institute of Information Security

Offense – Destination IP



Destination IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Source(s)	Last Event/Flow	Events/Flows
172.25.1.87		Net-10-...	No	Unknown	Unknown	0	2	1	1m 5s	41,454
10.2.8.1		Net-10-...	No	Unknown	Unknown	0	2	1	5m 59s	19,439
10.10.52.23		Net-10-...	No	Unknown	Unknown	0	2	1	4m 8s	2,749
192.168.1.11		Net-10-...	No	Unknown	Unknown	0	2	1	2m 45s	3,534
192.168.1.56		Net-10-...	No	Unknown	Unknown	0	2	1	2m 56s	3,090
192.168.0.105		Net-10-...	No	Unknown	Unknown	0	2	1	2m 45s	3,544
10.101.129.75		Net-10-...	No	Unknown	Unknown	0	2	1	2m 45s	3,716
192.168.0.101		Net-10-...	No	Unknown	Unknown	0	2	1	4m 38s	3,242
192.168.118.109		Net-10-...	No	Unknown	Unknown	0	2	1	3m 51s	3,076
192.168.0.23		Net-10-...	No	Unknown	Unknown	0	2	1	4m 34s	2,937
192.168.10.75		Net-10-...	No	Unknown	Unknown	0	1	1	8d 22h 52m ...	203
192.168.10.64		Net-10-...	No	Unknown	Unknown	0	1	1	8d 22h 52m ...	203
192.168.10.51		Net-10-...	No	Unknown	Unknown	0	1	1	8d 22h 52m ...	202
172.25.35.32		Net-10-...	No	Unknown	Unknown	0	2	2	8d 22h 52m ...	406
192.168.10.65		Net-10-...	No	Unknown	Unknown	0	1	1	8d 22h 52m ...	201
172.25.196.66		Net-10-...	No	Unknown	Unknown	0	1	1	8d 22h 52m ...	203
172.25.35.30		Net-10-...	No	Unknown	Unknown	0	1	1	8d 22h 52m ...	203
172.25.146.17		Net-10-...	No	Unknown	Unknown	0	1	1	8d 22h 52m ...	203
172.21.52.7		Net-10-...	No	Unknown	Unknown	0	1	1	8d 22h 52m ...	203
172.25.131.21		Net-10-...	No	Unknown	Unknown	0	2	2	8d 22h 51m ...	408
172.25.131.30		Net-10-...	No	Unknown	Unknown	0	2	2	8d 22h 51m ...	408
192.168.22.210		Net-10-...	No	Unknown	Unknown	0	1	1	8d 22h 51m ...	205

© Institute of Information Security

QRadar

User – User who is associated with this IP source address, If the User is not defined it remains Unknown

MAC – Mac address of source IP address

Host name – Host name associated with source IP address

Asset name – Asset name that is associated with source IP address

Weight – Relevance of the source Ip address, as defined by QRadar SIEM administrators in the Asset profile. Display 0 if profile doesn't exist

© Institute of Information Security

QRadar

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Networks –

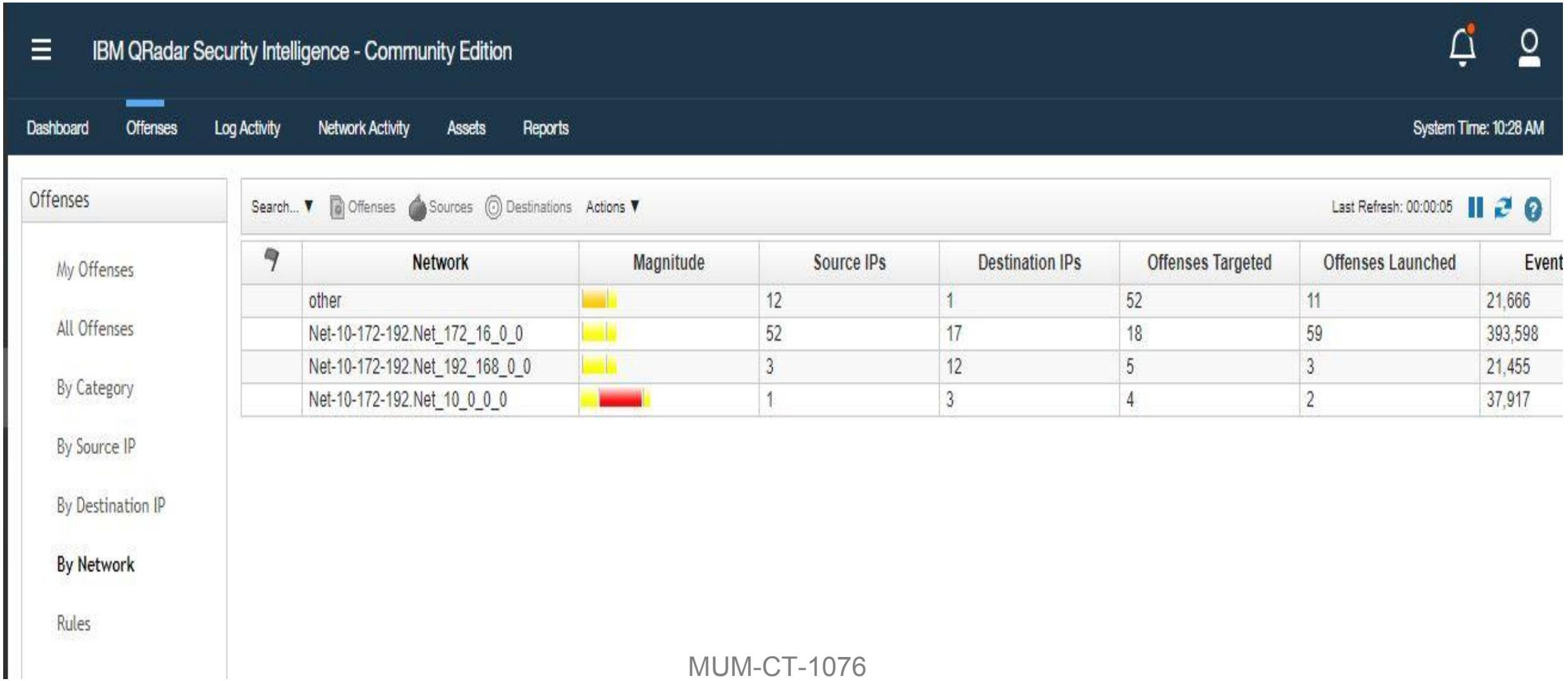
- All Networks declared within Admin Tabs are considered as Local Networks
- QRadar doesn't associate remote Networks is an Offense, even if they are specified as a Remote Network

Vulnerabilities

- If Local host has a vulnerability that could be Exploited into a attack, its noted in this parameter

© Institute of Information Security

Offense - Network



Network	Magnitude	Source IPs	Destination IPs	Offenses Targeted	Offenses Launched	Event
other		12	1	52	11	21,666
Net-10-172-192.Net_172_16_0_0		52	17	18	59	393,598
Net-10-172-192.Net_192_168_0_0		3	12	5	3	21,455
Net-10-172-192.Net_10_0_0_0		1	3	4	2	37,917

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Top 5 Source IP's

- QRadar SIEM displays the 5 addresses with the highest magnitude, which is where the suspected attack or policy breach originates.

© Institute of Information Security

Offense – Top 5 Source IP's

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Top 5 Source IPs Sources

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
63....		United States	No	Unknown	Unknown NIC	0	2	0	10m 17s	625
10.2...		Net-10-17...	No	Unknown	Unknown NIC	0	2	1	9m 5s	19,439
47....		United States	No	Unknown	Unknown NIC	0	2	0	13m 40s	1,250
202...		India	No	Unknown	Unknown NIC	0	2	0	18m 42s	1,250

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Top 5 Destination IP's

- QRadar SIEM displays the 5 local IP address based on magnitude which were targeted. Eg: Targets of ICMP scan

© Institute of Information Security

Offense – Top 5 Destination IP's

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Top 5 Destination IPs — Destinations

Destin... IP	Magnitude	Location	Vulnerability	Chained	User	MAC	Weight	Offenses	Source(s)	Last Event/Flow	Events/Flows
10.2...		Net-10-1...	No	No	Unknown	Unknown NIC	0	2	1	9m 5s	19,439

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Top 5 Log sources

- Top 5 major log sources are grouped and displayed under this
- If a Firewall provided information regarding multiple Firewall denies, this firewall is a major Log source.

© Institute of Information Security

Offense – Log sources

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Top 5 Source IPs

Sources

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
63....		United States	No	Unknown	Unknown NIC	0	2	0	10m 17s	625
10.2...		Net-10-17...	No	Unknown	Unknown NIC	0	2	1	9m 5s	19,439
47....		United States	No	Unknown	Unknown NIC	0	2	0	13m 40s	1,250
202...		India	No	Unknown	Unknown NIC	0	2	0	18m 42s	1,250

Top 5 Destination IPs

Destinations

Destin... IP	Magnitude	Location	Vulnerability	Chained	User	MAC	Weight	Offenses	Source(s)	Last Event/Flow	Events/Flows
10.2...		Net-10-1...	No	No	Unknown	Unknown NIC	0	2	1	9m 5s	19,439

Top 5 Log Sources

Log Sources

Name	Description	Group	Events	Offenses	Total Events
Fortigate@192.168.22.45			12,014	2	22,564

Top 5 Users

Users

Name	Events/Flows	Offenses	Total Events/Flows

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Top 5 Users

- QRadar SIEM lists the 5 users with the most events contributing to the offense

© Institute of Information Security

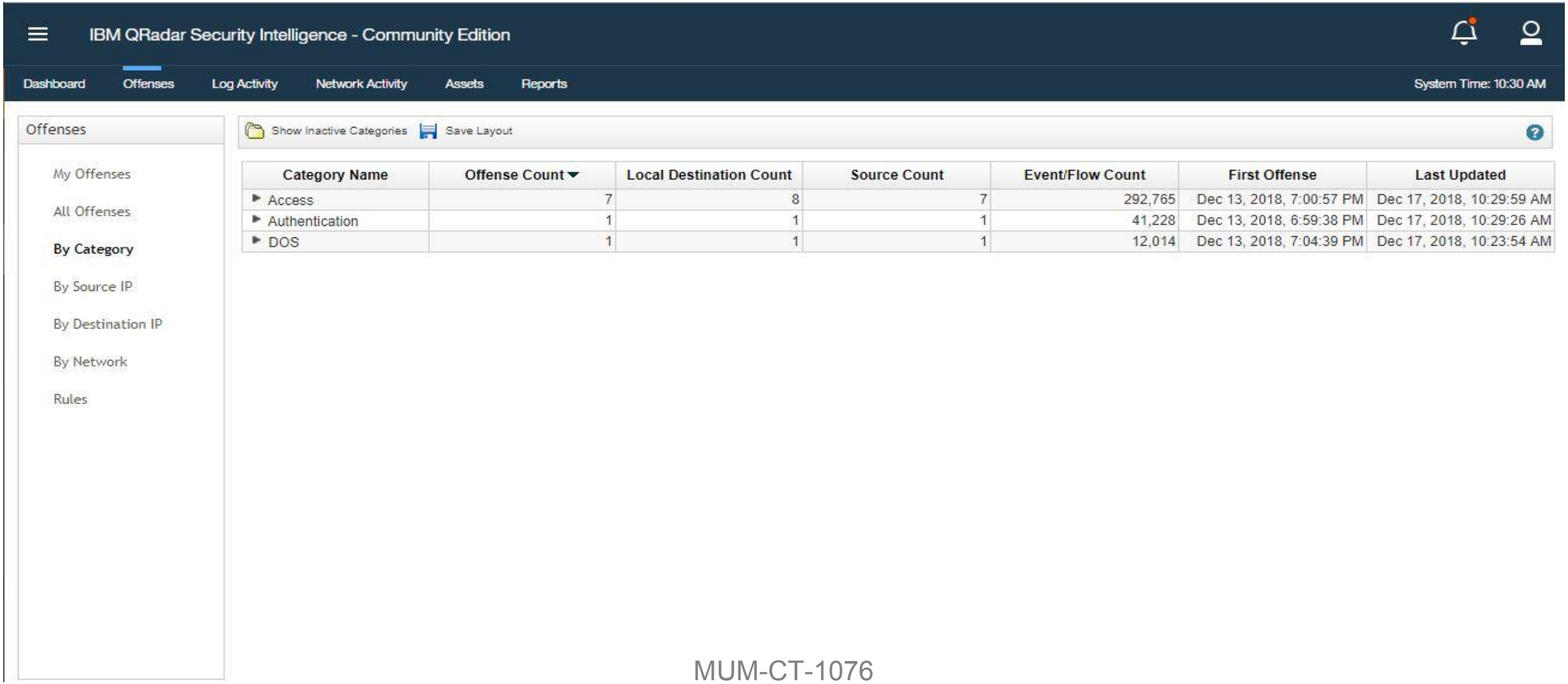
NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Top 5 Categories

- Consider a example, QRadar SIEM categorized most events into IDS Alert category, This is termed as a major category

© Institute of Information Security

Offense - Category



Category Name	Offense Count	Local Destination Count	Source Count	Event/Flow Count	First Offense	Last Updated
Access	7	8	7	292,765	Dec 13, 2018, 7:00:57 PM	Dec 17, 2018, 10:29:59 AM
Authentication	1	1	1	41,228	Dec 13, 2018, 6:59:38 PM	Dec 17, 2018, 10:29:26 AM
DOS	1	1	1	12,014	Dec 13, 2018, 7:04:39 PM	Dec 17, 2018, 10:23:54 AM

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Last 10 Events

- The Latest 10 Events are displayed to provide the Analyst information about development in the offense

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Last 10 flows

- The latest 10 flows are displayed to provide information regarding development in Network activities

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Annotations

- Annotations provide insights into why QRadar SIEM considers the event or observed Threatning
- QRadar SIEM can add annotations when it adds an offense

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Assessment of a Offense

- Display – To view Offense details
- Follow-up – Select if you wish to revisit offense later
- Hide – Hide offense details, remember QRadar will keep recording details regarding it.
- Protect – Prevents QRadar from deleting the offense, after retention period
- Close – Once resolved, offense could be closed
- Assign – Delegate the Offense to another User

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Investigating Events of an Offense

- Initially we need to Navigate and List the Target Events
- So In Offense Summary check Events and double-click to check Event information

© Institute of Information Security

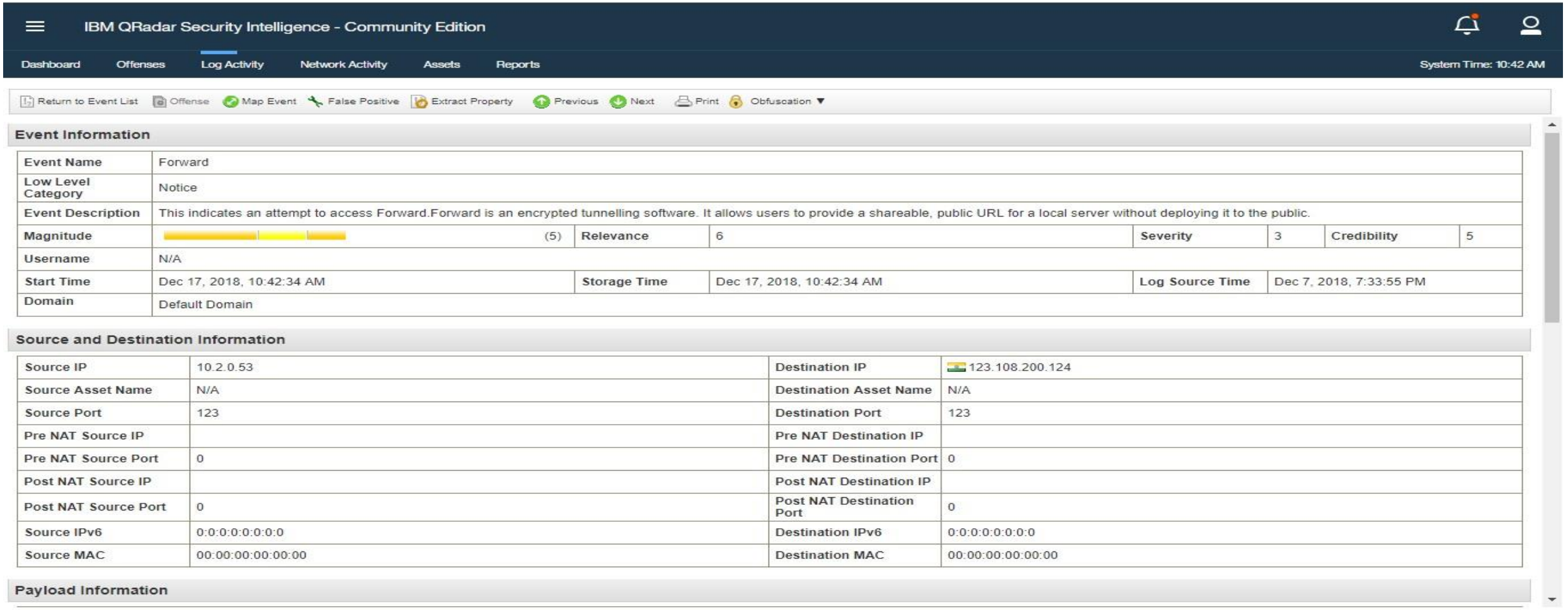
NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Event Details

- Start Time – The Time when QRadar SIEM received raw event from log source
- Storage Time – The period for which QRadar stored the Normalized event in Node
- Log Source Time – The time that is recorded in the Raw Event

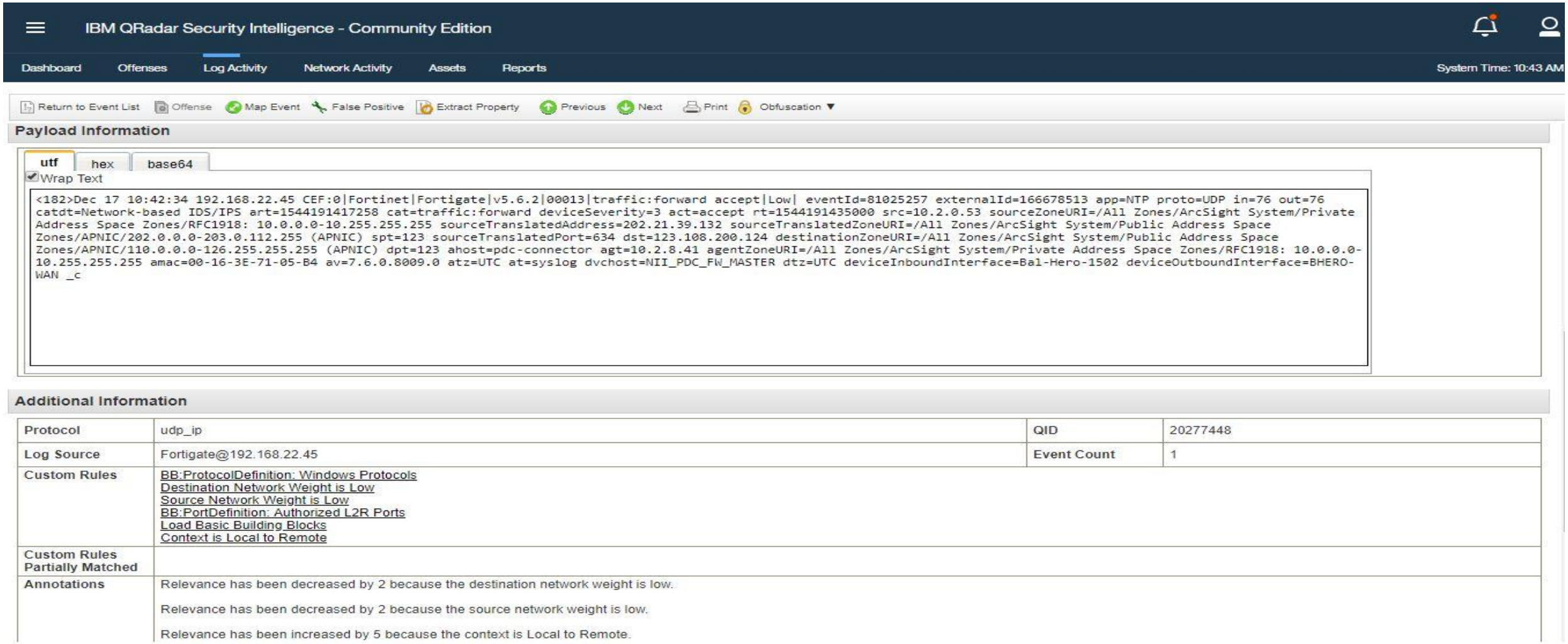
© Institute of Information Security

Event Information



© Institute of Information Security

Event Payload



© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Reviewing the Raw event

- QRadar pulls out Information from Raw events and Normalises it, including
  - Date
  - Time
  - Source IP address
  - Destination IP address
  - Protocol

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Additional Details

- **Protocol** – Provides information regarding Protocol being used
- **QID** – A Unique ID assigned by QRadar, used as an identifier for normalizing Events.
- **Log source** - Any System on network is a Log Source for QRadar
- **Event Count** – QRadar can enable or disable coalesce of multiple similar raw events into one normalized event. Event count resembles how many raw events have been coalesced into one Normalized event/

© Institute of Information Security

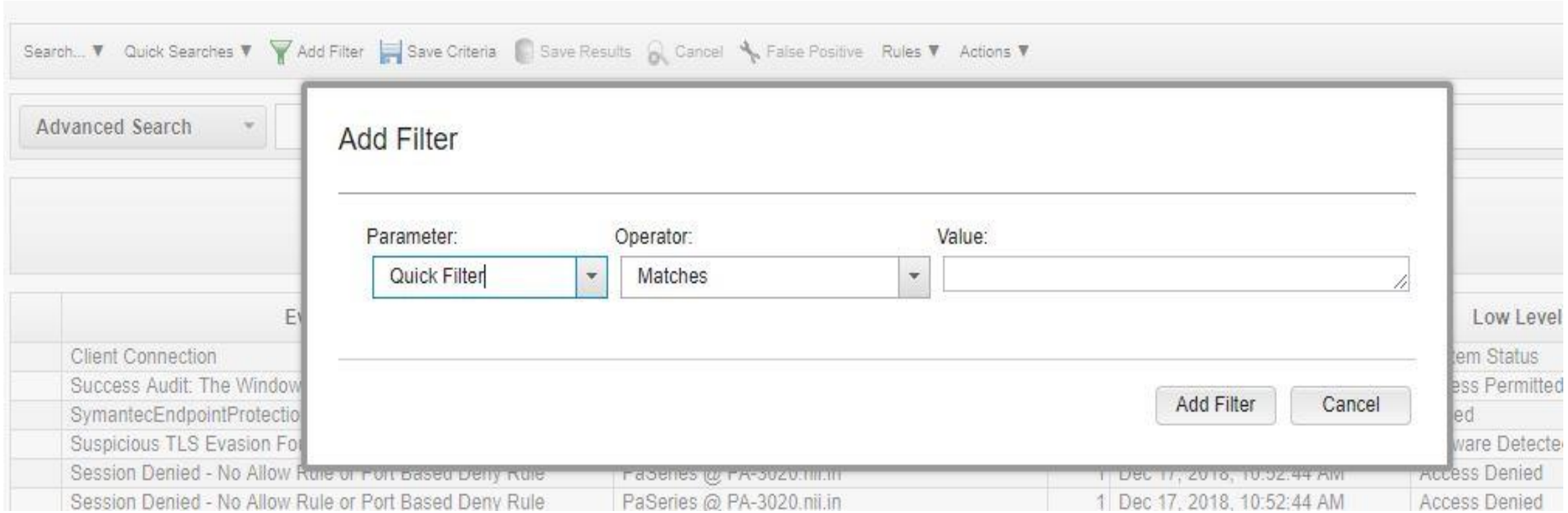
NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Use of Filters

- Within List of Events, filters could be applied for further offense analysis
- Right-click and choose pre-existing filters/remove filters if any
- You can choose a Time period, for which a filter will be applied.
- Click on Clear Filter to retrieve all events.

© Institute of Information Security

Add a Filter



© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Quick Filters

- Supports “And” , “Or” and “Not”.
- Can be used to filter out details from payload of a raw event.

© Institute of Information Security

Practical Session

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

MUM-CT-1076
TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Using grouping

- You can choose to Group Events based on Category, Protocol, Username, Log source, Source port, Custom rule etc
- By default QRadar SIEM displays Normalized Events for grouping
- Also you could choose to Real-time stream grouped and sorted events, or Last interval (refreshes every minute) which shows details of events last minute

© Institute of Information Security

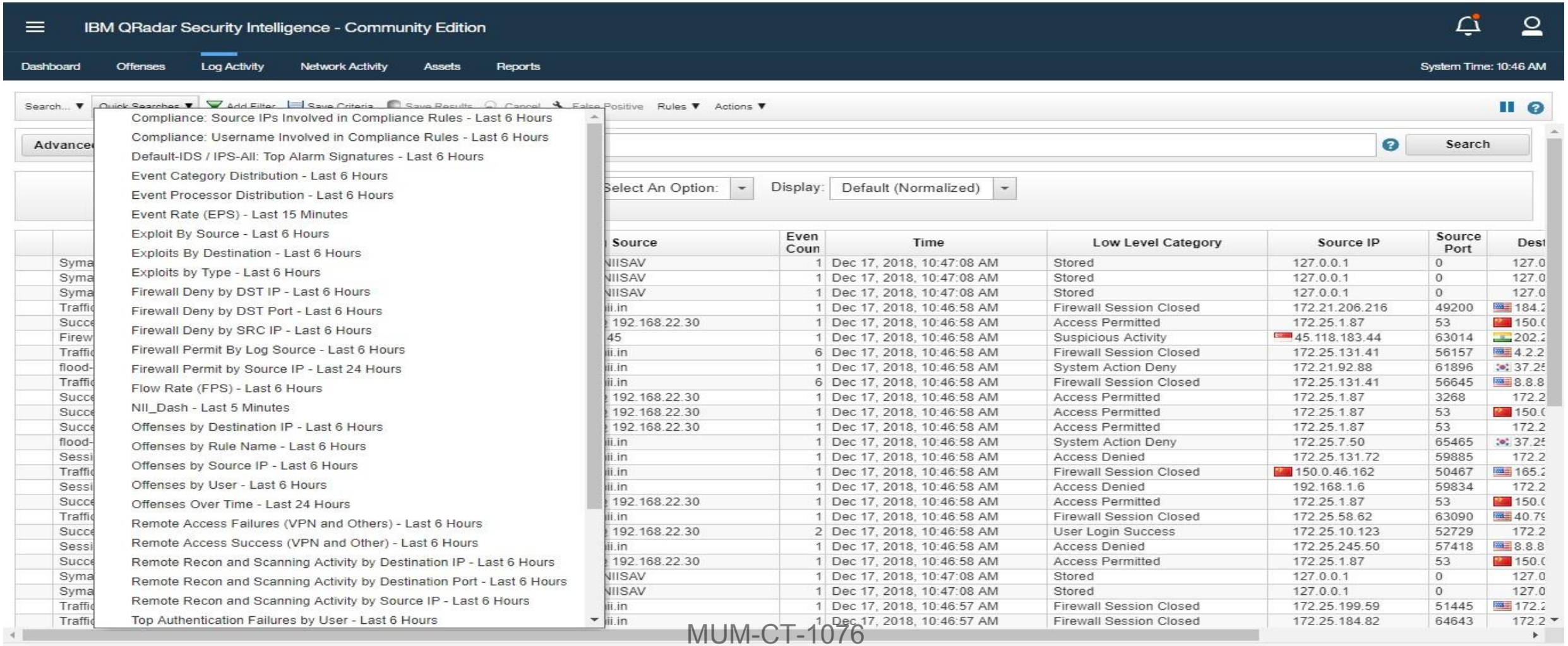
NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Searches

- Event lists always display result based on some default search.
- QRadar supports creating and saving a custom search, for investigative purposes
- The search parameters could be group name, Time, Category, etc
- You could also save you searches based on criteria's such as
  - Manage groups – Modify search groups
  - Include in Quick Searches
  - Share with Everyone
  - Set as Default
  - Include in Dashboard

© Institute of Information Security

Quick Search


IBM QRadar Security Intelligence - Community Edition
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
System Time: 10:46 AM
Search...
Quick Searches
Add Filter
Save Criteria
Save Results
Cancel
False Positive
Rules
Actions
Search
Select An Option:
Display:
Default (Normalized)
Compliance: Source IPs Involved in Compliance Rules - Last 6 Hours
Compliance: Username Involved in Compliance Rules - Last 6 Hours
Default-IDS / IPS-All: Top Alarm Signatures - Last 6 Hours
Event Category Distribution - Last 6 Hours
Event Processor Distribution - Last 6 Hours
Event Rate (EPS) - Last 15 Minutes
Exploit By Source - Last 6 Hours
Exploits By Destination - Last 6 Hours
Exploits by Type - Last 6 Hours
Firewall Deny by DST IP - Last 6 Hours
Firewall Deny by DST Port - Last 6 Hours
Firewall Deny by SRC IP - Last 6 Hours
Firewall Permit By Log Source - Last 6 Hours
Firewall Permit by Source IP - Last 24 Hours
Flow Rate (FPS) - Last 6 Hours
NII_Dash - Last 5 Minutes
Offenses by Destination IP - Last 6 Hours
Offenses by Rule Name - Last 6 Hours
Offenses by Source IP - Last 6 Hours
Offenses by User - Last 6 Hours
Offenses Over Time - Last 24 Hours
Remote Access Failures (VPN and Others) - Last 6 Hours
Remote Access Success (VPN and Other) - Last 6 Hours
Remote Recon and Scanning Activity by Destination IP - Last 6 Hours
Remote Recon and Scanning Activity by Destination Port - Last 6 Hours
Remote Recon and Scanning Activity by Source IP - Last 6 Hours
Top Authentication Failures by User - Last 6 Hours
Source
Even Coun
Time
Low Level Category
Source IP
Source Port
Dest

© Institute of Information Security

QRadar

Once you save and include your custom search in quick searches, its accessible through quick search tab

You can edit quick search by right-clicking on it

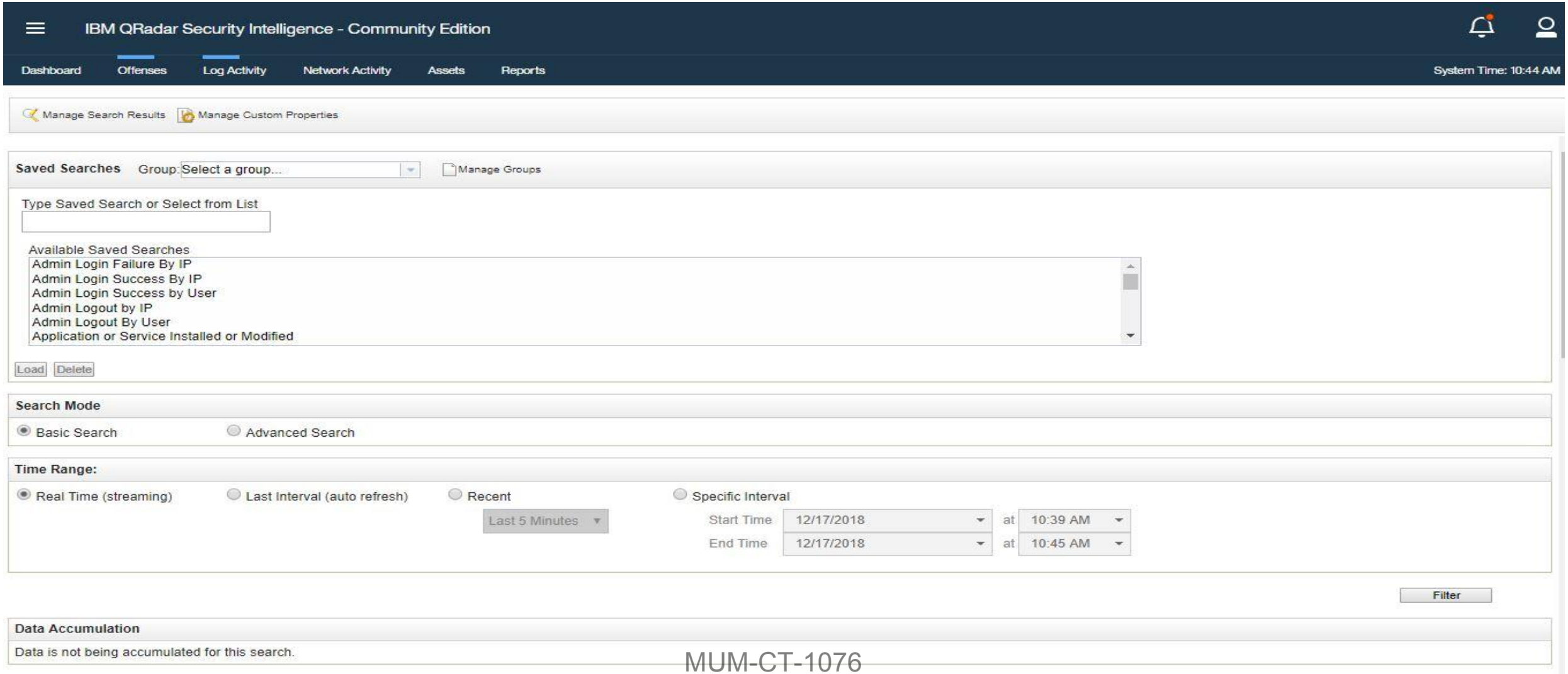
Manage search results provides option to save search results for auditing, (Delete) Delete previous/current search result, Cancel long-running searches or send a (Notify) Email when search finishes

Export option within Actions tab can be used to export search results in CSV or XML format if required

On Dashboard, you can click add item tab to add a saved search

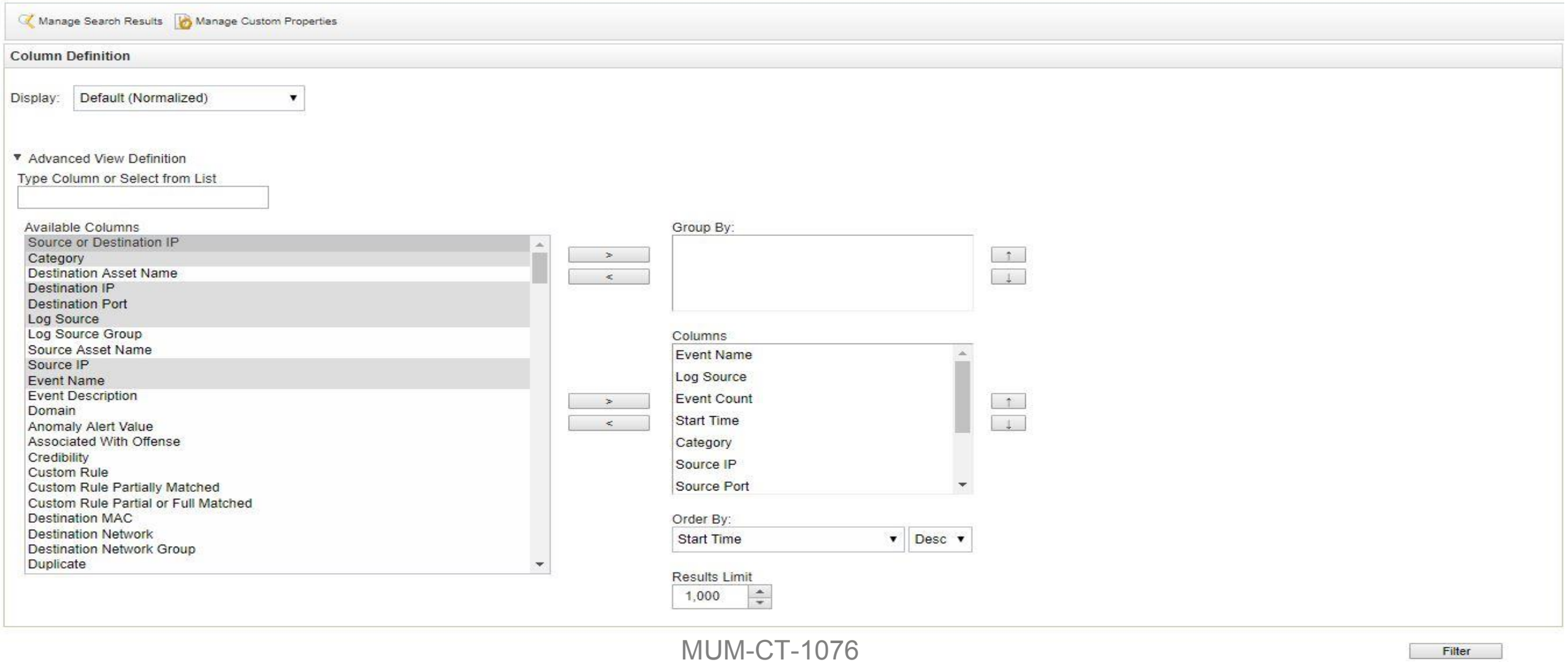
© Institute of Information Security

Using Search



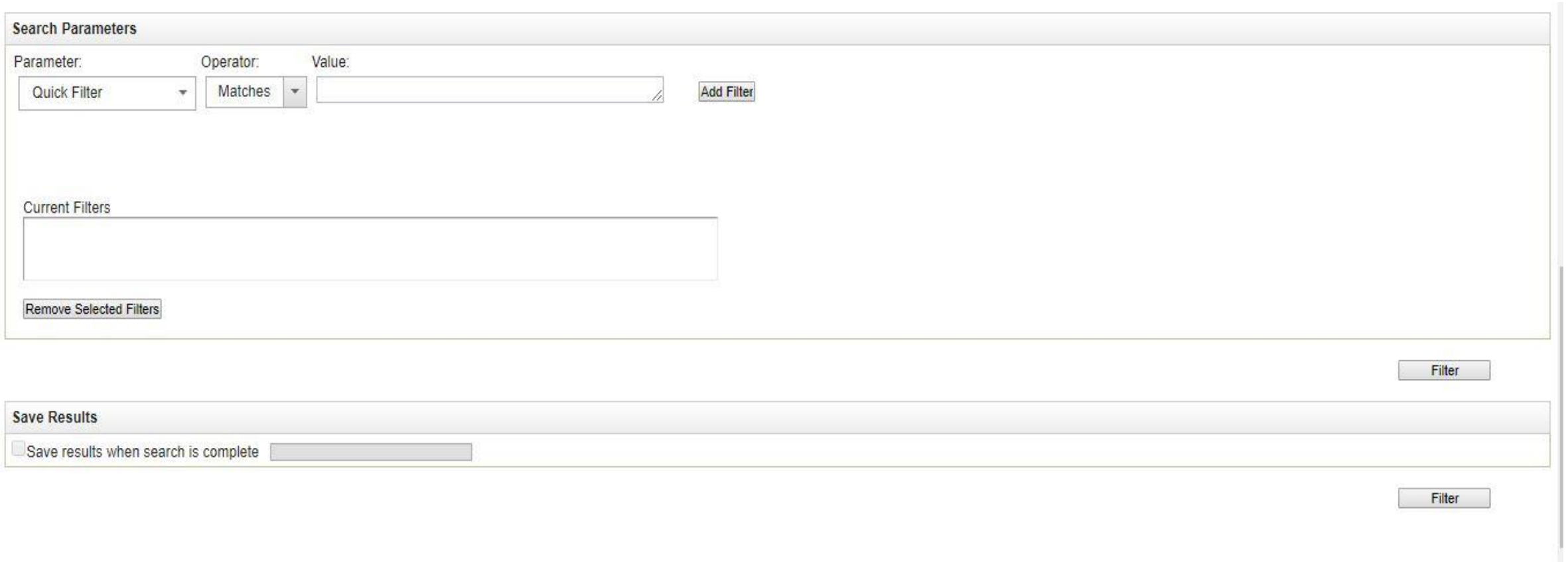
© Institute of Information Security

Customize search view



© Institute of Information Security

Create Search



© Institute of Information Security

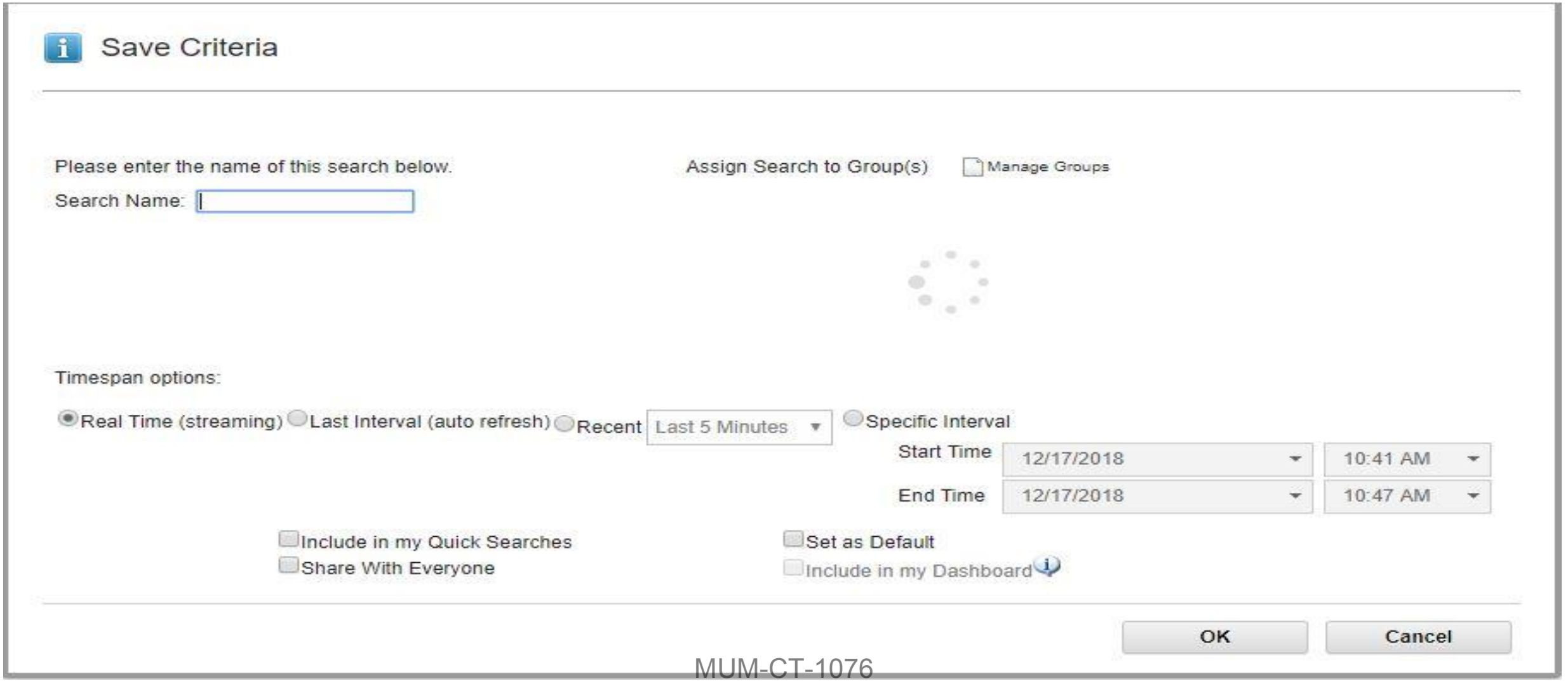
Practical session

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

MUM-CT-1076
TCS_SOC

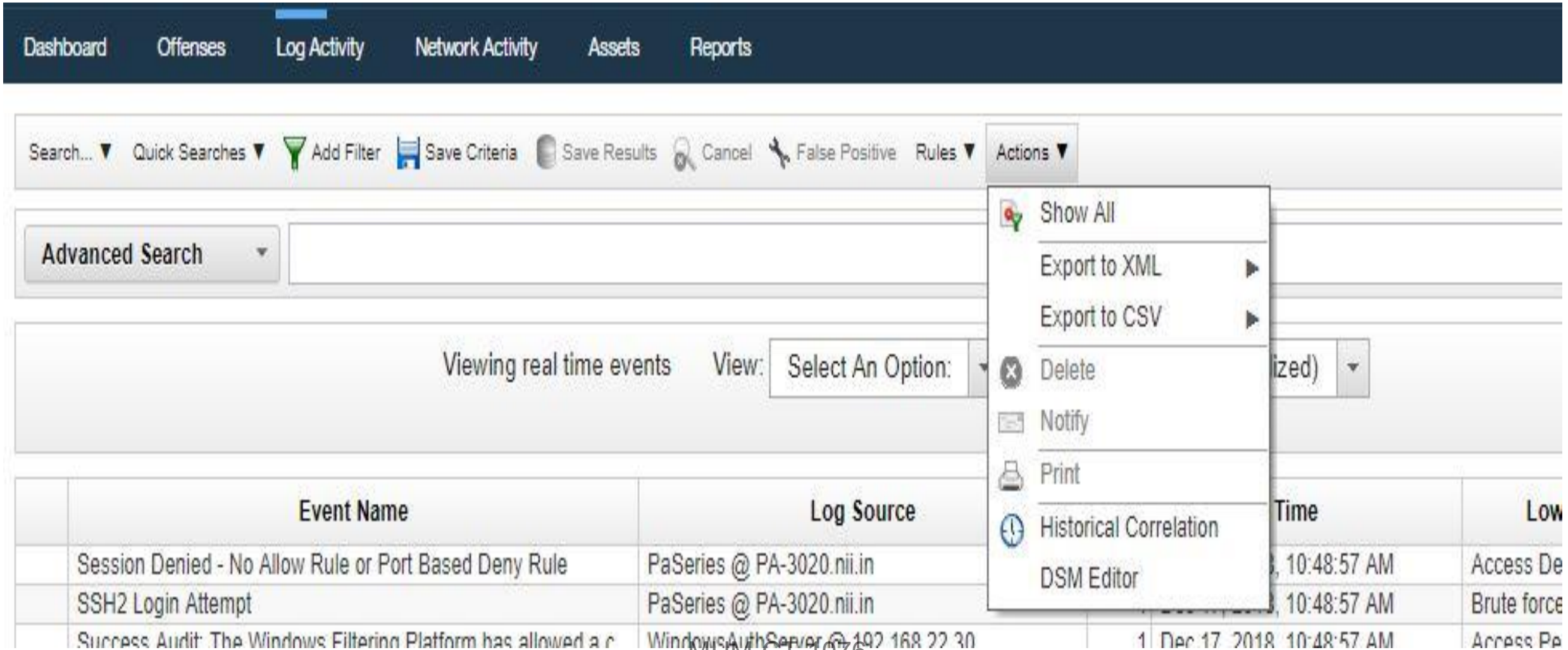
Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Save Search



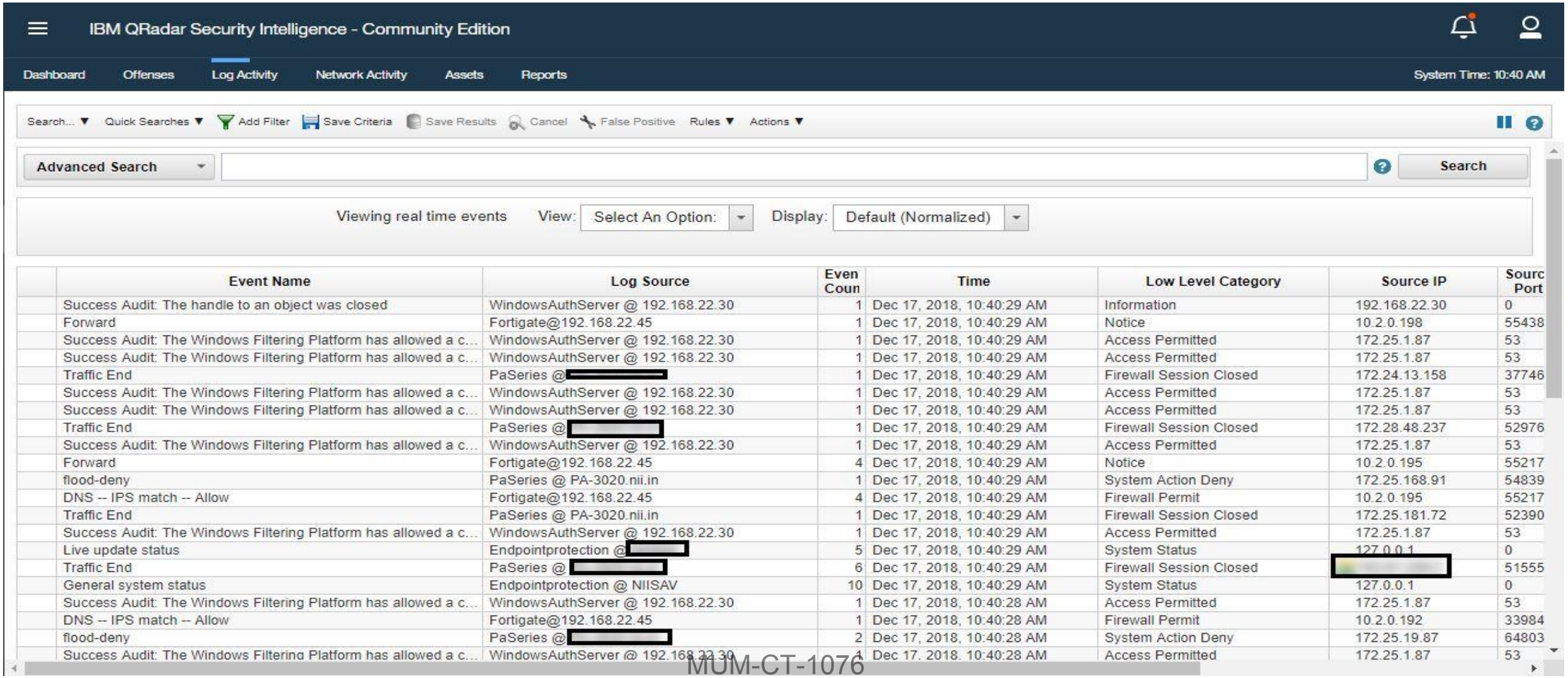
© Institute of Information Security

Export Search



© Institute of Information Security

Log Activity

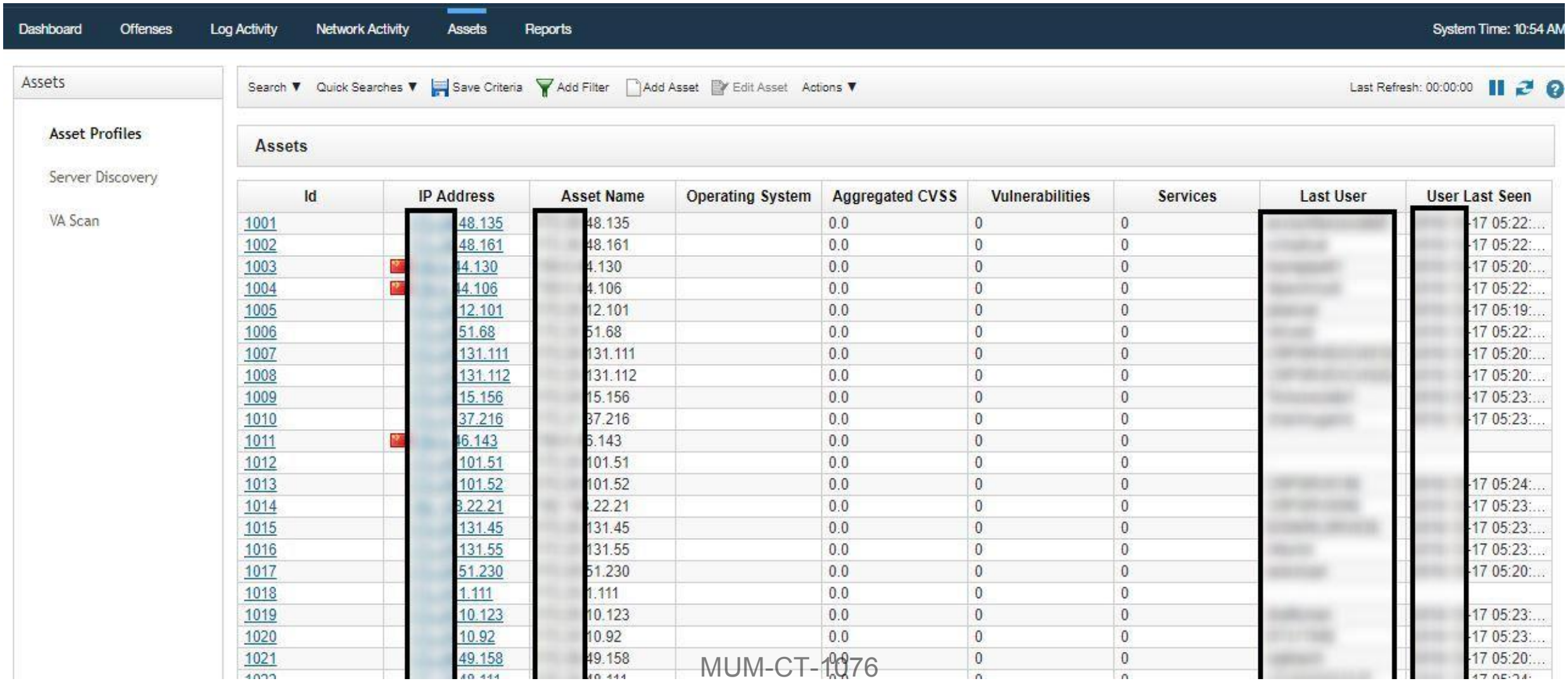


Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Sourc Port
Success Audit: The handle to an object was closed	WindowsAuthServer @ 192.168.22.30	1	Dec 17, 2018, 10:40:29 AM	Information	192.168.22.30	0
Forward	Fortigate@192.168.22.45	1	Dec 17, 2018, 10:40:29 AM	Notice	10.2.0.198	55438
Success Audit: The Windows Filtering Platform has allowed a c...	WindowsAuthServer @ 192.168.22.30	1	Dec 17, 2018, 10:40:29 AM	Access Permitted	172.25.1.87	53
Success Audit: The Windows Filtering Platform has allowed a c...	WindowsAuthServer @ 192.168.22.30	1	Dec 17, 2018, 10:40:29 AM	Access Permitted	172.25.1.87	53
Traffic End	PaSeries @[redacted]	1	Dec 17, 2018, 10:40:29 AM	Firewall Session Closed	172.24.13.158	37746
Success Audit: The Windows Filtering Platform has allowed a c...	WindowsAuthServer @ 192.168.22.30	1	Dec 17, 2018, 10:40:29 AM	Access Permitted	172.25.1.87	53
Success Audit: The Windows Filtering Platform has allowed a c...	WindowsAuthServer @ 192.168.22.30	1	Dec 17, 2018, 10:40:29 AM	Access Permitted	172.25.1.87	53
Traffic End	PaSeries @[redacted]	1	Dec 17, 2018, 10:40:29 AM	Firewall Session Closed	172.28.48.237	52976
Success Audit: The Windows Filtering Platform has allowed a c...	WindowsAuthServer @ 192.168.22.30	1	Dec 17, 2018, 10:40:29 AM	Access Permitted	172.25.1.87	53
Forward	Fortigate@192.168.22.45	4	Dec 17, 2018, 10:40:29 AM	Notice	10.2.0.195	55217
flood-deny	PaSeries @ PA-3020.nii.in	1	Dec 17, 2018, 10:40:29 AM	System Action Deny	172.25.168.91	54839
DNS -- IPS match -- Allow	Fortigate@192.168.22.45	4	Dec 17, 2018, 10:40:29 AM	Firewall Permit	10.2.0.195	55217
Traffic End	PaSeries @ PA-3020.nii.in	1	Dec 17, 2018, 10:40:29 AM	Firewall Session Closed	172.25.181.72	52390
Success Audit: The Windows Filtering Platform has allowed a c...	WindowsAuthServer @ 192.168.22.30	1	Dec 17, 2018, 10:40:29 AM	Access Permitted	172.25.1.87	53
Live update status	Endpointprotection @[redacted]	5	Dec 17, 2018, 10:40:29 AM	System Status	127.0.0.1	0
Traffic End	PaSeries @[redacted]	6	Dec 17, 2018, 10:40:29 AM	Firewall Session Closed	[redacted]	51555
General system status	Endpointprotection @ NIISAV	10	Dec 17, 2018, 10:40:29 AM	System Status	127.0.0.1	0
Success Audit: The Windows Filtering Platform has allowed a c...	WindowsAuthServer @ 192.168.22.30	1	Dec 17, 2018, 10:40:28 AM	Access Permitted	172.25.1.87	53
DNS -- IPS match -- Allow	Fortigate@192.168.22.45	1	Dec 17, 2018, 10:40:28 AM	Firewall Permit	10.2.0.192	33984
flood-deny	PaSeries @[redacted]	2	Dec 17, 2018, 10:40:28 AM	System Action Deny	172.25.19.87	64803
Success Audit: The Windows Filtering Platform has allowed a c...	WindowsAuthServer @ 192.168.22.30	1	Dec 17, 2018, 10:40:28 AM	Access Permitted	172.25.1.87	53

© Institute of Information Security

Asset List

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA



MUM-CT-1076
TCS_SOC

© Institute of Information Security

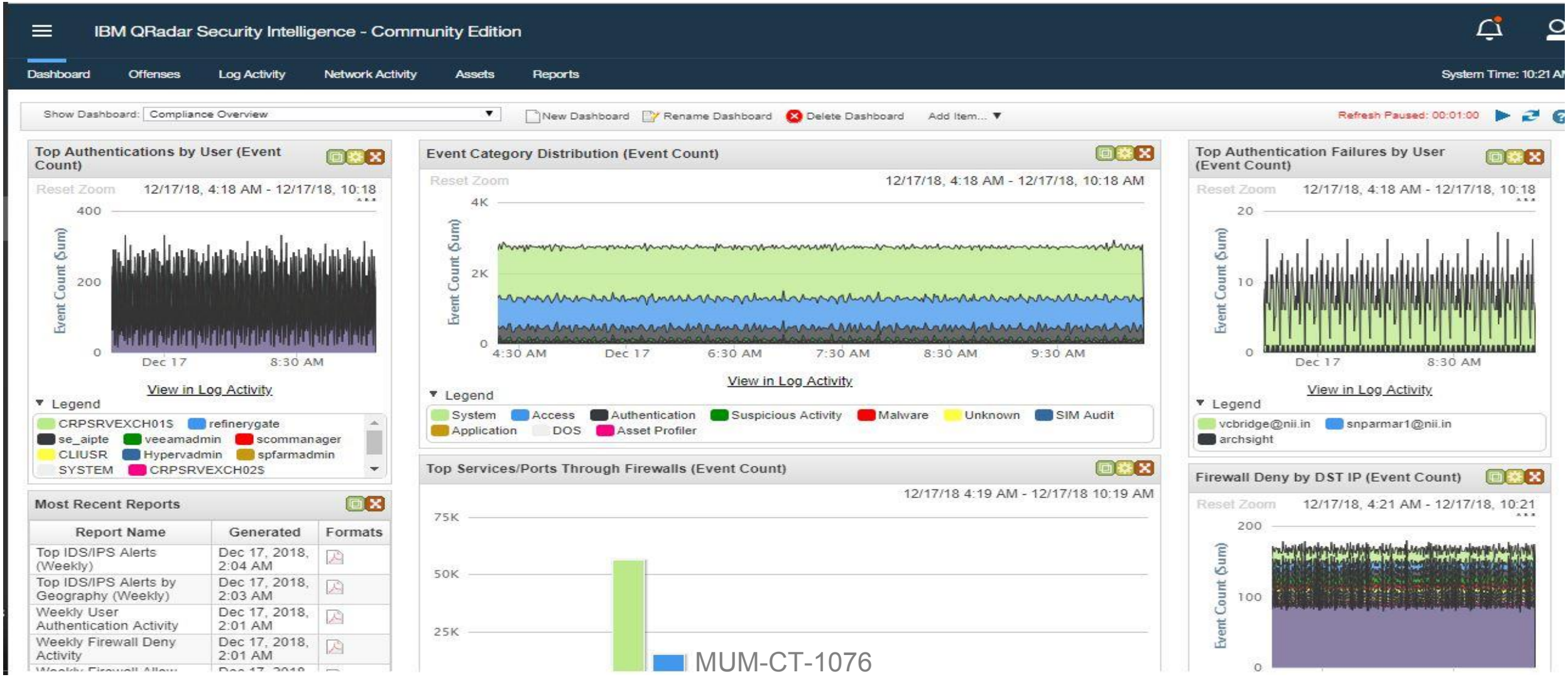
NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Dashboard

- QRadar provides a comprehensive Dashboard with ability to customize and create multiple Dashboards
- Dashboards provide brief and detailed information about multiple Entities
- Customization allows to keep/remove tabs, focusing on your organizations security
- Each Dashboard is associated to the specific user, So any changes to Dashboard doesn't affect other users
- Dashboard refreshes every minute, or you can also use pause and refresh

© Institute of Information Security

Dashboard



© Institute of Information Security

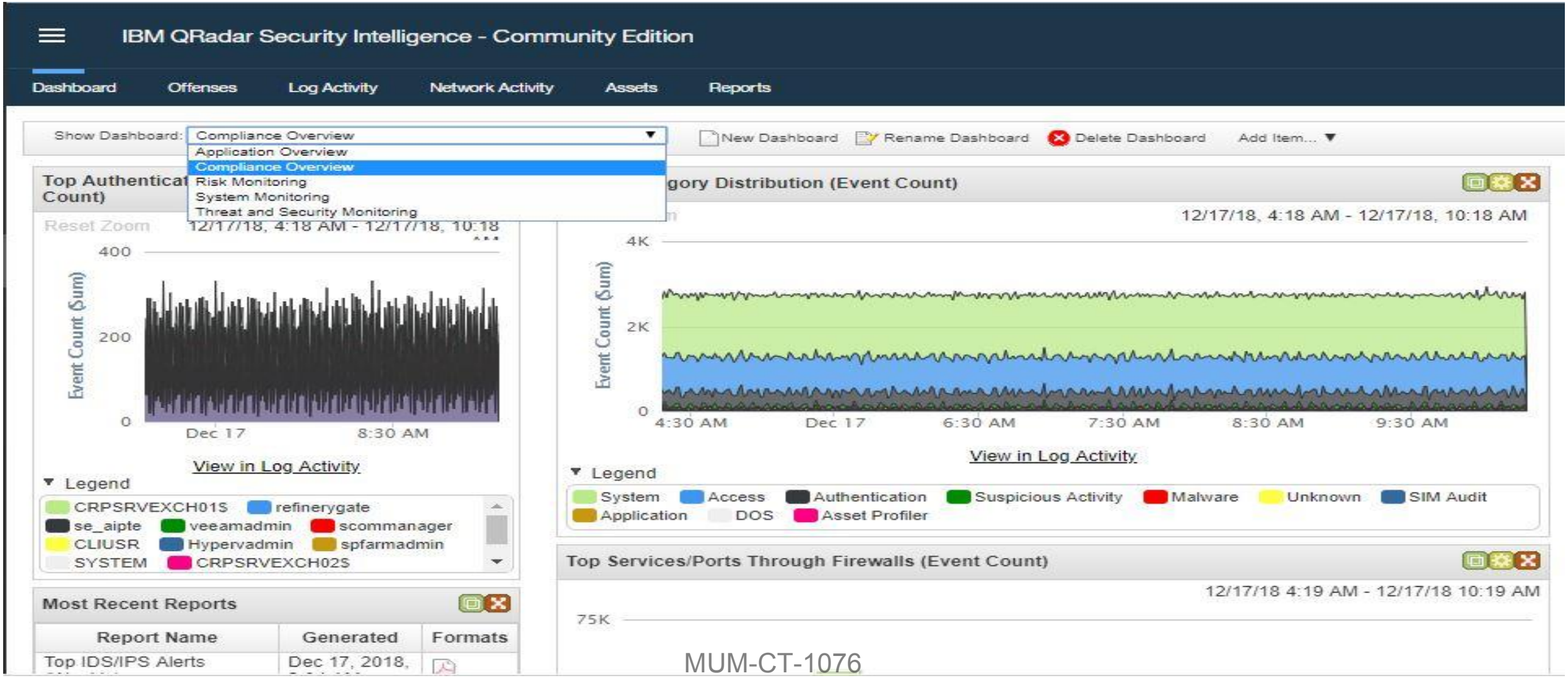
NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Default Dashboards

- Application Overview
- Compliance Overview
- Network Overview
- System Monitoring
- Threat and Security monitoring
- Virtual cloud Infrastructure
- Threat and Security Monitoring
- Vulnerability management

© Institute of Information Security

Dashboard



© Institute of Information Security

Analysis

Analysis Steps

- What was Detected by SIEM
- What is the Source
- What was detected by various Security devices
- Why Traffic Originated
- Activity at end point
- Activity at user
- What went out
- Mitre tactics
- Impact on environment

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Investigation

While investigation following point need to consider

- Identify the Start and End time of incident.
- Identify the Source (Source IP, Source port, domain, URL, Device name, Username, email)
- Identify the Destination (Destination IP, Destination port, domain used, URL, User, email)
- Perform the reputation check on IP, URL, Domain and email address.
- Correlate the IDS/IPS, EDR, AV, Firewall events for malicious process and traffic
- Correlate the email logs with the URL and process initiated.
- Check for process initiated by the malicious files.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Investigation

While investigation following point need to consider

- Identify any PowerShell and cmdlets initiated by malicious process or file
- Check for privileges tokens.
- Check for user creation and deletion process.
- Identify any file or script creation by malicious source.
- Identify if their sensitive information retrieval process initiated (PII,DB backup etc.)
- Check for third party geolocation.
- Identify suspicious connection for SSH/RDP/SMB/DNS.
- Check for traffic from source IP for malicious pattern activities.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Initial logging details

Logging details to be collected

- Source IP
- Source Port
- Source machine name
- Username
- User agent
- URL or domain
- Destination IP
- Destination port
- Sender email
- Receiver email
- File name

MUM-CT-1076
TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Initial logging details

Logging details to be collected

- File hash
- Sender domain
- Source and Destination Ip status
- URL or domain status
- Any outbound traffic detected for URL
- Antivirus EDR/HIDS detection
- Firewall/IPS detection
- Source of traffic

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Report Creation Session

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Practice Session

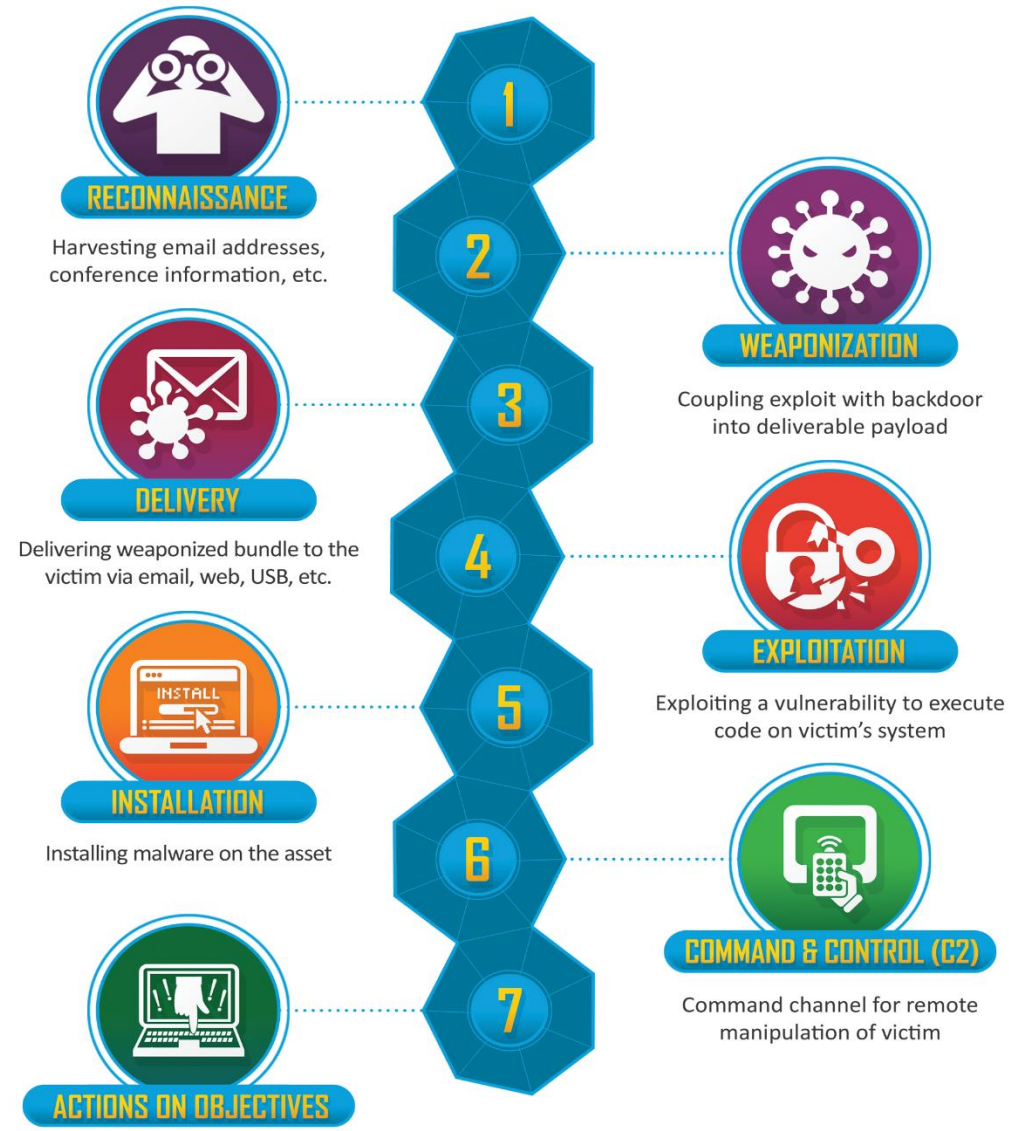
Point for Report

- IOC or logging details
- Explanation for incident
- Miter Mapping with remediation

MUM-CT-1076
TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Cyber Kill-Chain



MUM-CT-1076
TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE ATT$CK MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files		Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CM			Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Co			Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Co			Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Co			Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Co			Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	Co			Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Co			Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Ex			SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	Ex			Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Fil			Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	File System Logical Offsets		system information Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Gatekeeper Bypass		System Network Configuration Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	Hidden Files and Directories		System Network Connections Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	Hidden Users		System Owner/User Discovery				Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Hidden Window		System Service Discovery				Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	HISTCONTROL						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Image File Execution Options Injection						
	Signed Script Proxy Execution	Launch Agent								
	Source									
	Space after Filename									

MUM-CT-1076
TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

Reconnaissance (TA0043)

- The adversary is trying to gather information they can use to plan future operations.
- Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel.
- This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

Resource Development (TA0042)

- The adversary is trying to establish resources they can use to support operations.
- Resource Development consists of techniques that involve adversaries creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities.
- These resources can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using purchased domains to support Command and Control, email accounts for phishing as a part of Initial Access, or stealing code signing certificates to help with Defense Evasion.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

Initial Access (TA0001)

- The adversary is trying to get into your network.
- Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers.
- Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Execution (TA0002)

- The adversary is trying to run malicious code.
- Execution consists of techniques that result in adversary-controlled code running on a local or remote system.
- Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

Persistence (TA0003)

- The adversary is trying to maintain their foothold.
- Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.
- Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

Privilege Escalation (TA0004)

- The adversary is trying to gain higher-level permissions.
- Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives.
- Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

Examples of elevated access include:

  - SYSTEM/root level
  - local administrator
  - user account with admin-like access
  - user accounts with access to specific system or perform specific function

- These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

Defense Evasion (TA0005)

- The adversary is trying to avoid being detected.
- Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts.
- Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

Credential Access (TA0006)

- The adversary is trying to steal account names and passwords.
- Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping.
- Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

Discovery (TA0007)

- The adversary is trying to figure out your environment.
- Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act.
- They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective.
- Native operating system tools are often used toward this post-compromise information-gathering objective.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

Lateral Movement (TA0008)

- The adversary is trying to move through your environment.
- Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it.
- Reaching their objective often involves pivoting through multiple systems and accounts to gain. Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Collection (TA0009)

- The adversary is trying to gather data of interest to their goal.
- Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.
- Frequently, the next goal after collecting data is to steal (exfiltrate) the data. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

Command and Control (TA0011)

- The adversary is trying to communicate with compromised systems to control them.
- Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.
- There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

Exfiltration (TA0010)

- The adversary is trying to steal data.
- Exfiltration consists of techniques that adversaries may use to steal data from your network.
- Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

MITRE Attack Matrix

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Impact (TA0040)

- The adversary is trying to manipulate, interrupt, or destroy your systems and data.
- Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data.
- In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Creating Use Cases

Practical Session

MUM-CT-1076
TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Creating Playbook

- Cybersecurity playbooks can provide rapid automated response in several cybersecurity areas, including incident identification, incident detection, rapid response, and team communications.
- This ability to respond in real time elevates playbooks to an important place in your cyberdefense. The response can be reduced from hours (or days) to minutes.
- Automated cybersecurity playbooks are an automated guide for delivering a response to a cybersecurity event. They deploy and act across your entire network respond automatically to meet and stop cybersecurity threats.
- Standardized automated responses work.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Creating Playbook

- In context, the manual response to a cyber event requires that the SOC team manually brings up different security tools, gets various logs, and then likely runs an array of anti-virus/signature-based tools.
- In the meantime, an automated playbook runs the tools and counter-response automatically and then presents all of the data back to the SOC team. This saves time, reduces risk, and reduces costs – a win on all fronts.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Creating Playbook

- A good example of a simple automated playbook might be reviewing indicators of compromise (IOCs) to determine if a threat exists. Playbooks can be set up to automatically investigate an IP address, run a file against known threat intelligence sources, and more.
- This saves time and resources and provides security operations team personnel important actionable data sooner.
- Another example would center around the review and validation of anti-virus/anti-malware software alerts. The team can benefit from the early automated review and triage of these alerts to determine if they should be escalated and then actionable.
- Follow-on actions such as additional scanning can also be automated by the playbook.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Creating a Playbook

- Practical Session

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

NETWORK INTELLIGENCE

ISO 27001 CERTIFIED | PCI DSS QSA

Splunk

Introduction to Splunk

- Splunk was founded in 2003

- Splunk acquired Bugsense, a Mobile device data-analytics company in 2013 and Metafor, A company that implemented Machine learning to analyse data generated in IT infrastructure and Applications in 2015

- Splunk is one of the Leaders in SIEM globally according to Gartner

- In 2016, Google announced its cloud platform will integrate with Splunk to expand in areas like IT ops, security, and compliance.

- In 2019, Splunk announced new capabilities to its platform including the general availability of Data Fabric Search and Data Stream Processor.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

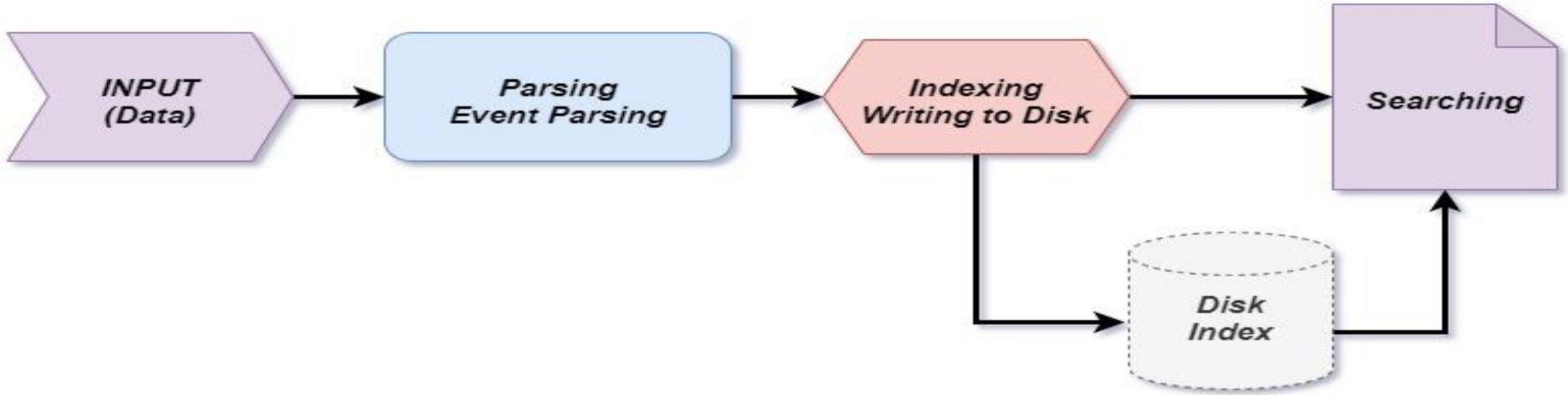
Introduction to Splunk

- Splunk Enterprise Security (ES) is a security information and event management (SIEM) solution that provides insight into machine data generated from security technologies such as network, endpoint, access, malware, vulnerability and identity information.

- Splunkbase is a community hosted by Splunk where users can go to find apps and add-ons for Splunk which can improve the functionality and usefulness of Splunk, as well as provide a quick and easy interface for specific use-cases and/or vendor products. As of October 2019, there were more than 2,000 apps available on the framework

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Splunk Architecture



Data Input Stage

- In this Stage Splunk software consumes the RAW Data stream from its source and breaks it into 64K blocks and annotates each block with Metadata keys. The Metadata keys include Hostname, Source and Source type of the data
- The Keys can also include value that are used internally, such as character encoding in the stream values that control processing of Data during the indexing stage, such as Index into which data should be stored.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Splunk Architecture

Data Storage stage

- In **Parsing phase**, Splunk Software examines, analyses and Transforms the data to extract only the relevant information. This is also known as event processing. It is during this phase that Splunk software breaks the data stream into individual events. The parsing phase has many sub-phases
  - Breaking the stream of Data into individual lines
  - Identifying parsing and setting Timestamps
  - Annotating individual events with metadata according to regex Transform rules

- In **Indexing phase** Splunk software writes parsed events to the index on the disk. It writes both the compressed raw data and the corresponding index file. The benefit of Indexing is that the data can be easily accessible during search.

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Splunk Architecture

Data **Searching** Stage

- This Stage controls how user accesses, views and uses the indexed data
- As part of the search function, the Splunk software stores user-created knowledge objects, such as reports, event types,
- Dashboards, Alerts and field extractors
- Search function also manages search process

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Splunk Components

There are 3 Main components in Splunk Architecture

- **Splunk Forwarder** – Used for Data Forwarding
- **Splunk Indexer** – Used for Parsing and Indexing Data
- **Search Head** – Is a GUI used for searching, analysing and reporting Data

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

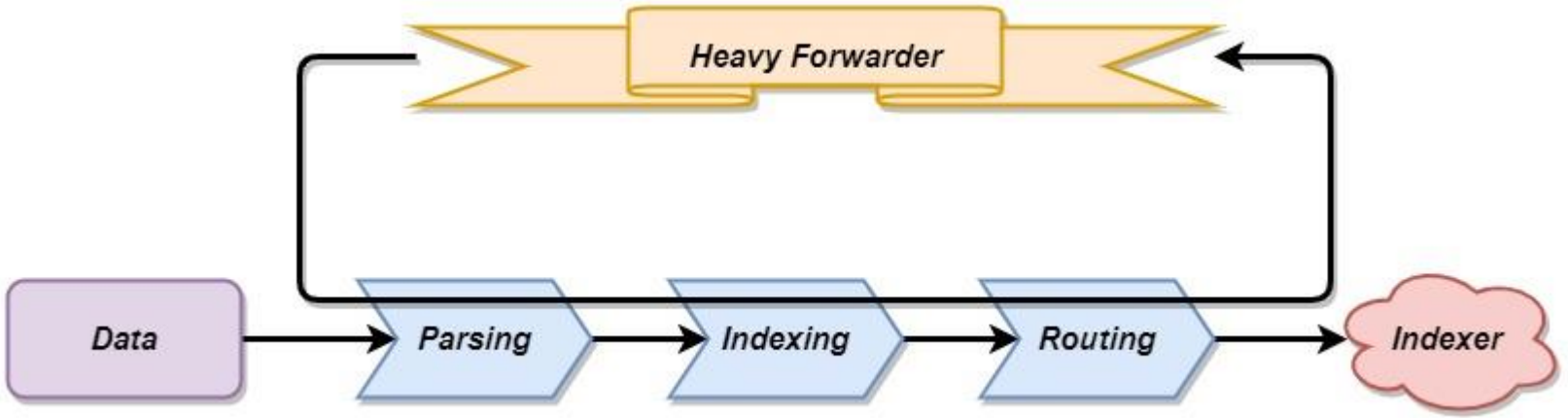
Splunk Components

Splunk Forwarder

Forwarder is a Agent deployed on End points to collect logs and sends them to indexer

Splunk has two types of Forwarder

- Universal Forwarder : Forwards the RAW data without any processing. This is fast and requires no processing power. At end point, but it ends up sending huge amount of RAW data to the Indexer
- Heavy Forwarder : Performs parsing and Indexing at source. Sends only parsed Information to Indexer



MUM-CT-1076
TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Splunk Components

Splunk Indexer

The Indexer transforms data into events, stores in to disk and adds it to an index, enabling searchability. The Indexer creates

The following files, separating them into directories called buckets

- Compressed Raw Data
- Indexes pointing to Raw Data
- Metadata files

The Indexer performs generic events processing on Log Data, such as applying timestamp and adding source, and can also execute user-defined transformation actions to extract specific information or apply special rules, such as filtering unwanted events

In Splunk Enterprise you can setup a cluster of indexers with replication between them, to avoid data loss and provide more system resources and storage space to handle large data volumes

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Splunk Components

Splunk Search Head

- The Search head provides the GUI for user to interact with Splunk
- It allows users to search and query Splunk data and Interfaces with Indexers to gain access to specific data the request
- Splunk provides a distributed search architecture, which allows you to scale up to handle large data volumes and better handle access control and geo-dispersed data.
- In a distributed search scenario, the search head sends search requests to a group of indexers also called search peers
- The Indexers perform the search locally and return results to the search head. Which merges the result and returns them to user

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Incident Response

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

2018, is the third decade since Morris worm threatened to plague the internet then. It also marks importance as first CERT was formed and eventually the importance of Incident Response was made evident.

Through the years the Threats have only gotten better, sophisticated, professional and for Monetary purpose.

The emerging APT and ML have just boosted the already professional Threat actors to be more stealthy and disruptive.

To add-on the weakest link of any Organization, Employees; are still unaware about this and unintentionally help such Threats.

© Institute of Information Security

Incident Response (IR)

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Incident Response is the capability of an Organization to handle a Incident and its impact, which ultimately has the goal of minimizing impact on business and managing Business continuity

Henceforth for this purpose Plans are designed which test the ability of Organization to be able to handle such incidents and minimize its impact on Business.

IR plans need to be revised to be able to achieve a optimal solution that meet the Goals.

© Institute of Information Security

Incident Response Plan

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Benefits

- To minimize the outcome of a Security Breach.
- Resume Business continuity.
- Improve general decision making of Organization.
- Standardized Procedure could be deployed effectively and quickly.
- Improves Co-ordination within and outside of an Organization
- Improves Third party relationships
- Implements security awareness within Organization

© Institute of Information Security

Preparation for IR

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Incident?

- Refers to an adverse event in an information system or network or the threat of the occurrence of such an event.
- Examples of Incident includes
  - Unauthorized use of another user's account
  - Unauthorized use of system privileges
  - Execution of malicious code that destroys data

© Institute of Information Security

Preparation for IR

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Terms

- Threat
- Vulnerability
- Exploit
- Risk Assessment

Risk = Likelihood x Impact

- **Likelihood:** The probability of an event occurring
- **Impact:** The amount of damage

© Institute of Information Security

Preparation for IR

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Actor

- Bad guy, Good guy
- External, Internal
- Incidental, Malicious

Negative Impact

- Expose
- Unauthorized Access
- Loss of Service
- Loss of data

© Institute of Information Security

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Asset

- Confidential Information
- Privileged Function or Business Functionality

© Institute of Information Security

Why do we handle Incidents?

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Limit damages

- Reputational & Brand Perception
- Loss of Competitive advantage

Guidance

- Ensuring operations staff take all necessary steps to resolve
- Executive level updates
- Ensure all incidents are closed properly

© Institute of Information Security

Why do we handle Incidents?

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Remediation activities

- Tactical: What is quick & easy to fix now?
- Strategic: How can we modify the environment to resolve long term?

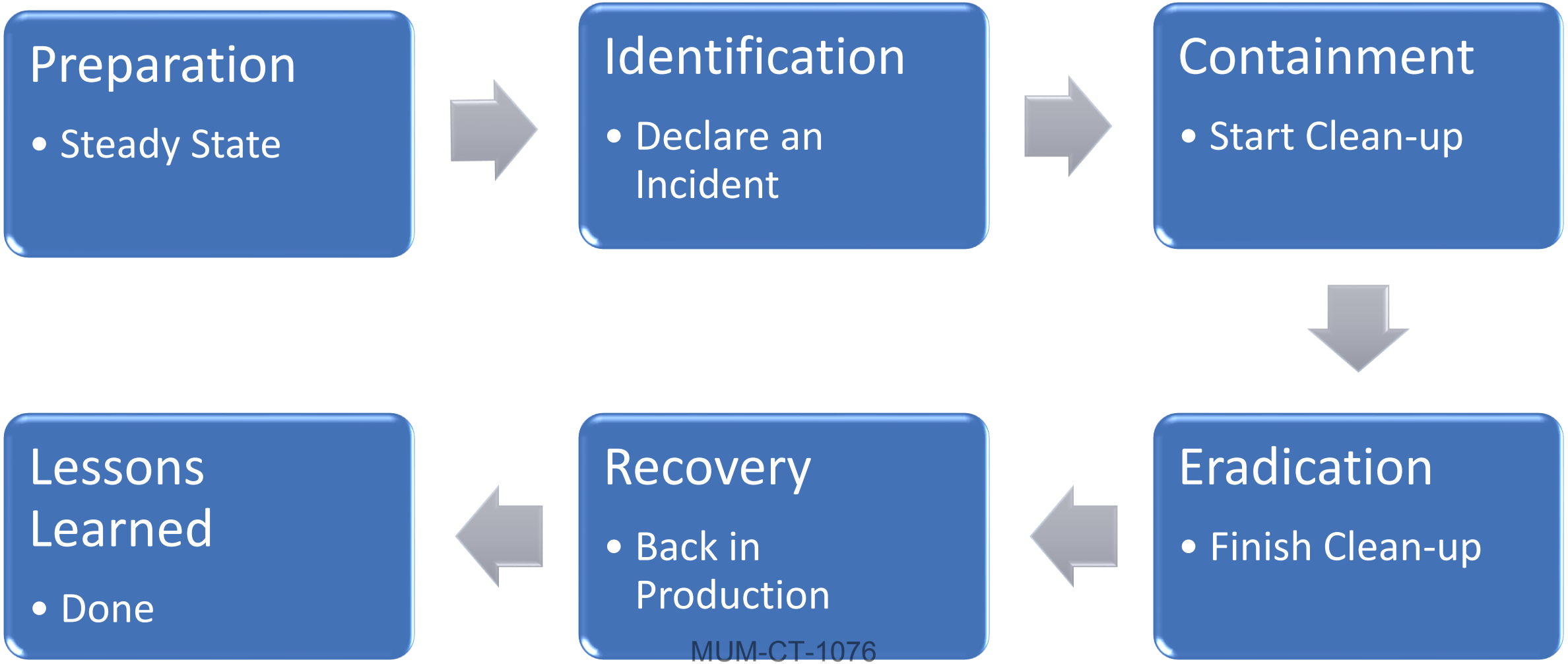
Education & Awareness

- Truth & clarity to executives
- A record of incidents that have been handled
- Increase understanding & knowledge of risk

© Institute of Information Security

Incident Response Handling.

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA



© Institute of Information Security

Incident Response Handling.

Different Organizations will have their own IR plans. Though no standard steps could be given for IR plans, mostly they will have the above Phases.

These phases may comprise of many steps, which are the actual methods to implement.

These steps may vary, elude, implement early or late, as per the Incident and Impact.

© Institute of Information Security

Preparation

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Goal

- People
- Policy
- Data
- Tools
- Communications
- Documentation

© Institute of Information Security

Preparation

Log Analysis Software	We have already seen few !!
Binary image creation software	**dd**,
	netcat & **ncat** for moving data across the network
Forensics software	**EnCase**
	Autopsy
	X-Ways Forensics Software

© Institute of Information Security

Preparation

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Tools

- **Wireshark**
- **Volatility**
- **Sysinternals**
- **TCPView**
- External Hard Drive (Imaging)
- Patch Cables

© Institute of Information Security

Identification

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Identification

- Here we recognize that a event has occurred and Authenticate the same.
- It’s important to perform Identification in initial stages for gaining information about incident and selecting respective steps.
- Maintain situational awareness
- Provide indications & warnings
- Provide current intelligence (up-to-date information)
- Enforce “a need to know” policy

© Institute of Information Security

Identification

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Network perimeter detection	• Identification occurs on network • Firewalls, Routers, WAF, IPS etc..
Host perimeter detection	• Identification occurs when data enters or leaves host • Local firewalls, IDS etc.
System Level Detection	• Identification happens based on activity on host itself

© Institute of Information Security

Identification

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Cheat sheets

- Processes & services
- Files
- Network Usage
- Scheduled Tasks
- Accounts
- Log Entries

© Institute of Information Security

Incident Recording

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Incident Recording

- It’s the initial immediate incident recording, which is analysed later for Incident remediation or Forensics.
- For example save all the Network packet traffic in form of pcap.
- Save all the incoming Logs.
- Backup all the existing records.
- In case of Virtual Machines save a Snapshot

© Institute of Information Security

Initial response

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Initial response

- Once the Incident is identified, The initial response can be chose based on minimizing the impact and retaining business continuity.
- For example in case of DoS attack, ISP provider could be contacted for assistance over traffic balancing.
- If computers may have been compromised, avoid using them for Incident Handling discussions
- Rely on out-of-band communications
  - Use telephones, mobile phones, faxes etc.
  - VOIP? Be careful if it’s not encrypted as it can be sniffed

© Institute of Information Security

Communicating the Incident

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Communicating the Incident

- It’s extremely important to release statement about Incident Publicly or Privately for awareness and quick response towards it.
- This also enables Third party and Government to provide assist
- GDPR has enacted the Security Breach law which enforces Organizations to release a statement of Breaches or Incidents within 72 hours.

© Institute of Information Security

Containment

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Put in place immediate controls to ensure the impact & possibility of propagation is minimized.

- Goal is stop the bleeding !
- Containment has several components
  - Short-Term Containment
  - Long-Term Containment

© Institute of Information Security

Containment – Quick actions

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

We need untainted evidence & can only get through image-creation

Short-term containment actions	Disconnect network cable
	Pull-the-plug ? (loses volatility memory & may damage drive)
	Using network management tools, isolate the system
	Apply filters on Firewalls

© Institute of Information Security

Containment – Long term

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Once we have got back up for our analysis, we can start making changes to system

Ideal: If the system can be kept offline, move to the Eradication phase

Less than Ideal, but sometimes necessary: If system must be kept in production, perform long term containment

© Institute of Information Security

Containment - Aftermath

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Long Term Containment Actions:

- Patch the system
- Change passwords
- Enhance security posture
- Delete accounts used by attacker
- Shutdown & remove backdoor processes

© Institute of Information Security

Formulating a Response Strategy

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

The Importance of effective Incident management for Organizational success is undisputed..

However, this process of formulating a response strategy will involve consideration of many internal and external factors.

Strategizing a plan for Incident Response, would be the base for any IR team

© Institute of Information Security

Formulating a Response Strategy

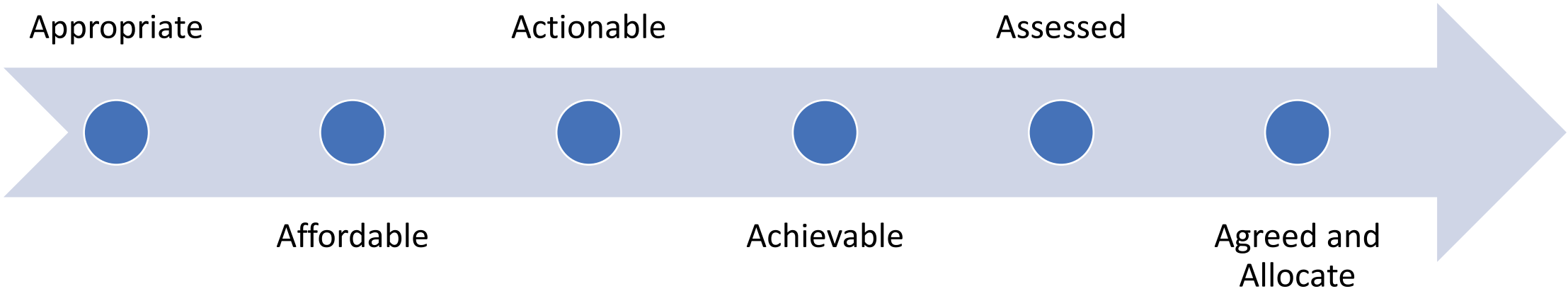
NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Pre-requisites

- List of Identified and Potential Incidents.
- Historical records of Organization
- List of Asset Registry and Human resource
- Financial resources and Post Incident Insurance
- SLA’s and third party agreement

© Institute of Information Security

Formulating a Response Strategy



© Institute of Information Security

Incident Classification

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Severity of Impact

- Critical Impact – Requires Immediate Real-Time resolution, assessment and treatment. Eg : Threat to backbone Infrastructure.
- High Impact – Requires serious attention and must be resolved within hours. Eg : Data Leakage
- Medium Impact – Fairly middle level impact and issue could be resolved within a day. Eg : User System crash.
- Low Impact – Lowest severity impact could be resolved within weeks. Eg : Network issues.

© Institute of Information Security

Incident Classification

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Based on the results from Identification and Containment the incident can be classified.

This would allow for quick remediation and eradication, ultimately minimizing the loss

There need to be pre-defined plans for some common incidents, so as to lower the response time.

© Institute of Information Security

Incident Classification

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Category

- Denial of Service
- Compromised Information
- Compromised Asset
- Unlawful Activity
- Internal Hacking
- External Hacking
- Malware
- Policy Violations… etc

© Institute of Information Security

Incident Investigation

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

- Incident Investigation is a term encompassing the Acquisition, Collection, Forensic, Report making, Archival etc
- The investigation seeks to determine the circumstances of the incident. Every incident will warrant or require an investigation.
- However, investigation resources like forensic tools, dirty networks, quarantine networks and consultation with law enforcement may be useful for the effective and rapid resolution of an emergency incident.
- In the fields of computer security and information technology, computer security incident management involves the monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events.
    - Read : https://en.wikipedia.org/wiki/Computer_security_incident_management

© Institute of Information Security

Data Collection

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Data Collection while Incident is ongoing or completed is a slow-moving task, thus preparing tools during preparation phase is recommended.

The Probability of Counter-Forensic techniques, adds up to the inefficiency of Data collection.

Data preservation before incident must be performed for relevant data rather than all data.

Data must be collected in a sophisticated manner to ease the Forensic and further process.

© Institute of Information Security

Data Collection

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

- Make forensics images of system as soon as is practical
- Grab an image of memory as well as file system
- Use blank media
- If possible, make a bit-by-bit image to get all file system data
- Not all incidents will allow you to take backup & analysis

© Institute of Information Security

Data Collection

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Further as a part of Social Engineering, Employee activity on Internal network which must be logged, needs to be analysed.

All the Logs must be centralized and if possible converted to a universal format for quick forensic Analysis.

Historical Archives, Logs and previous threat tackling process could be collected as a part of Data collection or preparation for assist.

© Institute of Information Security

Forensic Analysis

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Forensic Analysis is the phase within IR which could be carried out during ongoing incident(rarely the case) or is performed after resolving the incident.

This is due to the timeline of activities to perform during forensic analysis, it take a lot of TIME.

Also, unlike IR which prefers quick(almost real-time response); Forensic requires to process a lot of Information, Historical archives and variety of relevant Incidents to come up with a solution

© Institute of Information Security

Forensic Analysis

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

Most of Preparation for Forensic Analysis could be performed during Preparation phase such a Forensic toolkit, Historical archive centralization, Threat signatures, Threat containment and evidence collection.

Make a Chain-of-custody documentation.

Labelling and Transportation of evidence maintaining their integrity.

© Institute of Information Security

FTK Imager

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

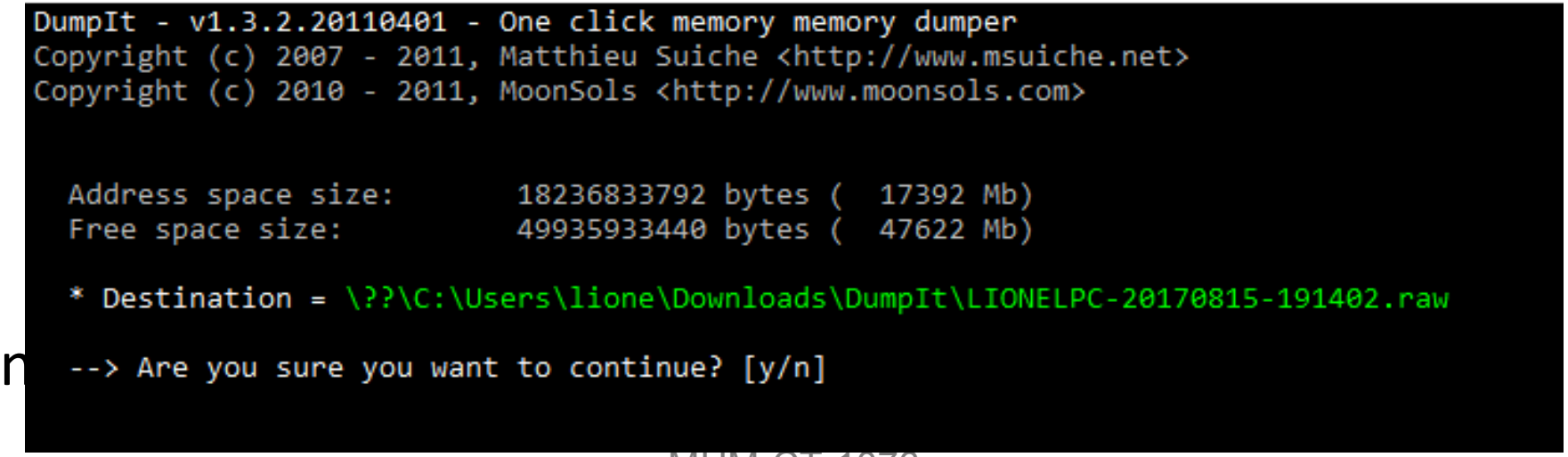
FTK Imager

- Create forensic images of local hard drives, CD-DVDs, entire folders, individual files or Usb
- Preview files & folders
- Preview the contents of forensic image stored
- Mount an image for read only view that leverages Windows Explorer to see the content of the image exactly as the user saw it in original drive
- Export files & folders from forensics image
- See & recover files that have been deleted from recycle bin, but not have been overwritten on the drive

RAM capture

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

- Memory Acquisition Tools
  - Belkasoft RAM Capturer
  - DumpIT
  - FTK Imager
- Memory An
  - Mandiant Redline
  - Volatility



Practical Session

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

MUM-CT-1076
TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.

Volatility

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

To view the OS info of the raw file enter the following command

vol.py <filename> imageinfo.

```
sansforensics@siftworkstation:/cases$ vol.py -f FORENSIC-65F3A7-20160419-084332.
raw imageinfo
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with Win
XPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/cases/FORENSIC-65F3A7-201604
19-084332.raw)
                      PAE type : PAE
                           DTB : 0x34c000L
                          KDBG : 0x80545be0
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000
             KUSER_SHARED_DATA : 0xffdf0000
           Image date and time : 2016-04-19 08:43:38 UTC+0000
     Image local date and time : 2016-04-19 14:13:38 +0530
sansforensics@siftworkstation:/cases$
```

Practical Session

NETWORK INTELLIGENCE
ISO 27001 CERTIFIED | PCI DSS QSA

MUM-CT-1076
TCS_SOC

Privileged & Confidential | ©2019, Network Intelligence Private Limited. All Rights Reserved.